

A Arquitetura de Resiliência Cibernética Helix:

*Articulando Formação Humana, Integração Operacional e Governança
ao Longo do Ciclo de Vida da Resiliência Cibernética*

Daniel Ferreira Porta

ORCID: 0009-0002-8002-5066

E-mail: dferreira@danresa.com.br

DANRESA Cybersecurity — São Bernardo do Campo, São Paulo, Brasil

DANRESA USA LLC — Miami, Flórida, Estados Unidos

Versão em Português do Brasil

Tradução autorizada do autor a partir do manuscrito original em inglês

*"The Helix Cyber Resilience Architecture: Articulating Human Formation, Operational Integration,
and Governance Across the Cyber Resilience Lifecycle"*

(SSRN — 2026)

Abril de 2026

Resumo

Este artigo apresenta a Arquitetura de Resiliência Cibernética Helix, uma arquitetura conceitual baseada em ciclo de vida que articula a resiliência cibernética como uma capacidade progressiva, desenvolvida ao longo de três dimensões interdependentes: formação humana, integração operacional e governança. Fundamentada em mais de duas décadas de prática profissional em segurança cibernética e na observação contínua de como a resiliência emerge em contextos reais, a Helix propõe uma perspectiva estruturada que complementa frameworks consolidados como o NIST Cybersecurity Framework 2.0, a ISO/IEC 27001:2022, o NICE Workforce Framework, os CSTA K-12 Standards e o ISACA COBIT.

A arquitetura é construída sobre estruturas fundacionais que sustentam a postura de cibersegurança ao longo do tempo, organizadas em três curvas de maturidade interdependentes — formativa, operacional e de governança — unificadas pela variável comum da maturidade do indivíduo em relação à exposição ao risco cibernético. Um modelo de cinco níveis, transversal às três curvas e fundamentado na redução observável do risco, oferece um meio estruturado de descrever a progressão desde a exposição fundacional até a liderança arquitetural. O artigo identifica ainda transições críticas entre as curvas como elementos arquiteturais específicos, cuja qualidade influencia a continuidade estrutural da resiliência cibernética ao longo do ciclo de vida.

A abordagem enfatiza a resiliência como uma capacidade em evolução, construída por meio da prática, da exposição a contextos reais e da progressão contínua. Em vez de substituir frameworks estabelecidos, a Helix oferece uma lente arquitetural complementar que permite observar a progressão da maturidade humana e institucional dentro do ecossistema de referências existentes. O artigo descreve também um ecossistema de implementação atualmente em desenvolvimento, que operacionaliza os princípios da arquitetura em contextos formativos, operacionais e de governança. Este trabalho constitui um modelo em desenvolvimento contínuo e é oferecido como um convite à reflexão, à aplicação, à crítica e ao refinamento por parte das comunidades acadêmicas e profissionais interessadas na continuidade estrutural da resiliência cibernética ao longo do tempo.

Palavras-chave: resiliência cibernética; arquitetura de cibersegurança; ciclo de vida; modelo de maturidade; formação humana; integração operacional; governança em cibersegurança; frameworks complementares; transições críticas; ecossistema de implementação.

Abstract

This paper presents the Helix Cyber Resilience Architecture, a conceptual lifecycle-based architecture that articulates cyber resilience as a progressive capability developed across three interdependent dimensions: human formation, operational integration, and governance. Grounded in more than two decades of professional practice in cybersecurity and in sustained observation of how resilience emerges in real-world contexts, Helix proposes a structured perspective that complements established frameworks such as the NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, the NICE Workforce Framework, the CSTA K-12 Standards, and ISACA COBIT.

The architecture is built upon foundational structures that sustain cybersecurity posture over time, organized into three interdependent maturity curves — formative, operational, and governance — unified by the common variable of the individual's maturity in relation to cyber risk exposure. A five-level model, transversal across the three curves and grounded in observable risk reduction, offers a structured means to describe progression from foundational exposure to architectural leadership. The paper further identifies critical transitions between curves as specific architectural elements, whose quality influences the structural continuity of cyber resilience across the lifecycle.

The approach emphasizes resilience as an evolving capability, built through practice, real-world exposure, and continuous progression. Rather than replacing established frameworks, Helix offers a complementary architectural lens that enables the progression of human and institutional maturity to be observed across the ecosystem of existing references. The paper also describes an implementation ecosystem currently under development, which operationalizes the architecture's principles in formative, operational, and governance contexts. This work constitutes an ongoing developmental model and is offered as an invitation to reflection, application, critique, and refinement by the academic and professional communities interested in the structural continuity of cyber resilience over time.

Keywords: cyber resilience; cybersecurity architecture; lifecycle; maturity model; human formation; operational integration; cybersecurity governance; complementary frameworks; critical transitions; implementation ecosystem.

1. Introdução

1.1 Motivação e Origem

A resiliência cibernética tornou-se um conceito cada vez mais central no campo da segurança da informação. À medida que organizações, instituições e sociedades se tornam mais dependentes de infraestruturas digitais, a capacidade de antecipar, resistir, recuperar-se e adaptar-se a ameaças cibernéticas emerge como um requisito estratégico. Frameworks consolidados — como o NIST Cybersecurity Framework, a ISO/IEC 27001, o NICE Workforce Framework, os CSTA K-12 Computer Science Standards e o ISACA COBIT — moldaram o entendimento atual desse campo, abordando, respectivamente, funções organizacionais, sistemas de gestão, competências profissionais, padrões educacionais e estruturas de governança.

Entretanto, a resiliência cibernética não se desenvolve apenas pela implementação de controles, pela aquisição de competências ou pela adoção de práticas de governança. Ela se desenvolve ao longo de um ciclo de vida que articula a formação humana, a prática operacional e a tomada de decisão estratégica ao longo do tempo. A continuidade entre essas dimensões raramente é abordada explicitamente pelos frameworks existentes, cada um dos quais tende a se concentrar em uma camada específica do ecossistema de cibersegurança.

Ao longo de mais de duas décadas de experiência em operações de segurança cibernética, o autor observou que a emergência efetiva da resiliência depende substancialmente da continuidade estrutural entre o modo como os indivíduos são formados, o modo como os profissionais integram seus comportamentos em ambientes operacionais e o modo como os tomadores de decisão situam o risco cibernético no processo decisório estratégico. Essas observações revelaram, progressivamente, padrões arquiteturais que, quando articulados de forma sistemática, ofereceram uma perspectiva estruturada sobre o ciclo de vida da resiliência cibernética.

A Arquitetura de Resiliência Cibernética Helix emergiu dessa observação continuada. Em vez de propor um novo conjunto de controles, competências ou processos de governança, ela oferece uma perspectiva arquitetural que conecta os elementos já definidos pelos frameworks consolidados, organizando-os em torno da continuidade estrutural da resiliência cibernética ao longo do ciclo de vida humano e institucional.

1.2 Lacuna Abordada pelo Artigo

O ecossistema de frameworks em cibersegurança alcançou notável maturidade em suas respectivas dimensões. O NIST CSF oferece uma referência funcional para a cibersegurança organizacional. A ISO/IEC 27001 estrutura sistemas de gestão de segurança da informação. O NICE Framework define competências de força de trabalho. Os CSTA Standards estabelecem diretrizes educacionais. O COBIT articula a governança de TI com objetivos corporativos.

Apesar dessa robustez em cada dimensão, a articulação entre elas ao longo do ciclo de vida permanece como um domínio em que perspectivas arquiteturais sistemáticas são comparativamente menos desenvolvidas. A literatura e a prática em cibersegurança frequentemente tratam essas dimensões como domínios paralelos, abordados por iniciativas e frameworks distintos, em vez de tratá-las como camadas interconectadas de uma arquitetura mais ampla de resiliência.

Este artigo aborda essa lacuna ao propor uma perspectiva arquitetural explicitamente baseada em ciclo de vida, complementar aos frameworks existentes e orientada à continuidade estrutural entre formação humana, integração operacional e governança. A Arquitetura de Resiliência Cibernética Helix é oferecida não como substituta de referências estabelecidas, mas como uma lente complementar que permite observar e articular a progressão da maturidade humana e institucional ao longo do ecossistema de frameworks.

1.3 Contribuições do Artigo

Seis contribuições principais derivam da proposta apresentada neste artigo. A primeira é a fundamentação conceitual da Helix como arquitetura, baseada em quatro princípios arquiteturais — centrada no humano, progressiva, arquiteturalmente integrada e mensurável. A segunda é a descrição de três curvas de maturidade interdependentes — formativa, operacional e de governança — unificadas pela variável comum da maturidade do indivíduo em relação à exposição ao risco cibernético. A terceira é um modelo de maturidade em cinco níveis, transversal às três curvas e fundamentado na redução observável do risco. A quarta é a identificação de transições críticas entre as curvas como elementos arquiteturais específicos. A quinta é a apresentação de domínios de aplicação para a arquitetura. A sexta é a descrição de um ecossistema de implementação atualmente em desenvolvimento, que operacionaliza os princípios da arquitetura em contextos reais.

1.4 Organização do Artigo

Após esta introdução, a Seção 2 revisa os frameworks consolidados em cibersegurança que constituem o ecossistema de referência no qual a Helix se situa. A Seção 3 apresenta a fundamentação conceitual da arquitetura, incluindo seus princípios e sua relação com os frameworks existentes. A Seção 4 desenvolve as três curvas de maturidade que estruturam a arquitetura. A Seção 5 apresenta o modelo de maturidade de cinco níveis aplicável às três curvas. A Seção 6 aborda as transições críticas entre as curvas como elementos arquiteturais. A Seção 7 discute domínios de aplicação para a arquitetura. A Seção 8 desenvolve as formas específicas de integração complementar entre a Helix e cada um dos frameworks consolidados. A Seção 9 descreve o ecossistema de implementação atualmente em desenvolvimento. A Seção 10 apresenta as considerações finais, incluindo limitações reconhecidas e direções para pesquisas futuras.

2. Fundamentação: Frameworks Estabelecidos

Esta seção apresenta os principais frameworks consolidados em cibersegurança que constituem o ecossistema de referência no qual a Arquitetura de Resiliência Cibernética Helix se situa. Cada framework é descrito em termos de seu escopo, de sua estrutura central e de sua contribuição primária para o campo da cibersegurança. O objetivo não é oferecer uma revisão exaustiva de cada referência, mas estabelecer as bases conceituais sobre as quais se assentará a articulação complementar proposta nas seções subsequentes.

2.1 NIST Cybersecurity Framework (NIST CSF)

O NIST Cybersecurity Framework, desenvolvido pelo National Institute of Standards and Technology, constitui uma das referências mais amplamente adotadas em cibersegurança organizacional. Em sua versão 2.0, lançada em 2024, o framework estrutura as atividades de cibersegurança em torno de seis funções centrais — Govern (Governar), Identify (Identificar), Protect (Proteger), Detect (Detectar), Respond (Responder) e Recover (Recuperar) — que, em conjunto, descrevem as atividades essenciais para a gestão de risco cibernético em organizações de diferentes portes e setores.

Cada função é subdividida em categorias, subcategorias e referências informativas que possibilitam aplicação adaptativa em diferentes contextos organizacionais. A introdução da função Govern na versão 2.0 incorpora explicitamente a dimensão de supervisão organizacional — abrangendo o estabelecimento, a comunicação e o monitoramento de estratégias, expectativas e políticas de cibersegurança —, refletindo o reconhecimento crescente de que a cibersegurança é inseparável do processo decisório estratégico e da prestação de contas organizacional.

O NIST CSF oferece um vocabulário comum e uma estrutura organizada para a cibersegurança, permitindo que as organizações avaliem sua postura atual, definam estados-alvo e desenvolvam planos de melhoria. Sua perspectiva funcional e estrutural constitui referência fundamental para a articulação arquitetural proposta na Helix.

2.2 ISO/IEC 27001:2022

A ISO/IEC 27001, em sua versão 2022, estabelece os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI), oferecendo uma estrutura de gestão baseada em uma abordagem orientada a riscos com ciclo de melhoria contínua. A norma é amplamente

adotada como referência para certificação formal, conformidade regulatória e alinhamento contratual em ambientes corporativos e governamentais.

O SGSI estruturado pela ISO/IEC 27001 abrange a definição de políticas de segurança da informação, a identificação e o tratamento de riscos, a implementação de controles de segurança (referenciados no Anexo A, alinhado à ISO/IEC 27002) e o monitoramento e melhoria contínuos do sistema. A lógica orientada a riscos e o ciclo de melhoria contínua constituem elementos centrais da norma, refletindo o entendimento de que a segurança da informação não é uma condição estática, mas uma capacidade gerenciada que requer atenção contínua.

A contribuição da ISO/IEC 27001 para o campo consiste na sistematização formal da segurança da informação como sistema de gestão. Essa formalização é particularmente relevante para a articulação arquitetural proposta pela Helix, que reconhece a dimensão estrutural da cibersegurança e a importância da progressão contínua na manutenção da resiliência ao longo do tempo.

2.3 NICE Workforce Framework for Cybersecurity

O NICE Workforce Framework for Cybersecurity, desenvolvido pela National Initiative for Cybersecurity Education (NICE) sob os auspícios do NIST, estabelece uma taxonomia abrangente de competências, conhecimentos, habilidades e papéis de trabalho em cibersegurança. O framework oferece uma linguagem comum para empregadores, educadores e profissionais descreverem, desenvolverem e avaliarem capacidades em cibersegurança.

A estrutura central do NICE organiza as capacidades em cibersegurança em categorias de competências, áreas de especialidade, papéis de trabalho e tarefas, conhecimentos e habilidades associadas. Essa estrutura possibilita a articulação entre programas educacionais, trajetórias profissionais e iniciativas de desenvolvimento de força de trabalho, oferecendo referência para o desenvolvimento sistemático de profissionais de cibersegurança.

A contribuição do NICE Framework para o campo consiste na representação estruturada da dimensão humana da cibersegurança, com ênfase particular nas competências e papéis necessários ao exercício efetivo das funções profissionais. Essa dimensão humana se articula às curvas formativa e operacional da Helix, estabelecendo conexões entre a descrição de competências oferecida pelo NICE e a perspectiva arquitetural sobre progressão de maturidade proposta neste artigo.

2.4 CSTA K-12 Computer Science Standards

Os CSTA K-12 Computer Science Standards, desenvolvidos pela Computer Science Teachers Association, estabelecem diretrizes para o ensino de ciência da computação desde a primeira infância até o ensino médio. Os padrões organizam conceitos fundamentais em áreas como Sistemas Computacionais, Redes e Internet, Dados e Análise, Algoritmos e Programação, e Impactos da Computação.

Entre as dimensões abordadas, os padrões cobrem explicitamente a cibersegurança, a privacidade digital, a ética computacional e a cidadania digital. Essa cobertura reflete o reconhecimento de que competências fundamentais em cibersegurança devem ser desenvolvidas desde a educação básica, como parte integrante da formação digital dos estudantes, em vez de serem abordadas exclusivamente em contextos pós-secundários especializados.

A contribuição dos CSTA Standards para o campo consiste no tratamento estruturado da dimensão formativa inicial da cibersegurança. Essa dimensão educacional é particularmente relevante para a curva formativa da Helix, que aborda o desenvolvimento pré-operacional de comportamentos e consciência em cibersegurança.

2.5 ISACA COBIT

O ISACA COBIT, em sua versão 2019, oferece um framework para a governança e a gestão de TI corporativa, articulando princípios de governança, objetivos de gestão, práticas e processos que sustentam o alinhamento entre a tecnologia da informação e os objetivos de negócio. O COBIT inclui dimensões específicas relacionadas à cibersegurança e à gestão de riscos, o que o torna particularmente relevante para organizações que integram a cibersegurança em estruturas mais amplas de governança corporativa.

A estrutura central do COBIT organiza a governança e a gestão de TI em torno de objetivos de governança e gestão, cada qual sustentado por processos, estruturas organizacionais, fluxos de informação e componentes de cultura, ética e comportamento. Essa estrutura possibilita a integração entre estratégia de TI, objetivos corporativos e cibersegurança, oferecendo referência para a articulação entre essas dimensões em contextos organizacionais complexos.

A contribuição do COBIT para o campo consiste na representação estruturada da dimensão de governança da cibersegurança, com ênfase particular em sua articulação com

objetivos corporativos mais amplos. Essa dimensão de governança se articula à curva de governança da Helix, estabelecendo conexões entre a perspectiva estrutural oferecida pelo COBIT e a perspectiva arquitetural sobre maturidade decisória proposta neste artigo.

2.6 Síntese: Um Ecossistema de Referências Complementares

Os frameworks descritos nas subseções anteriores constituem, em conjunto, um ecossistema de referências que aborda dimensões distintas da cibersegurança: o NIST CSF aborda funções organizacionais; a ISO/IEC 27001 aborda o sistema de gestão; o NICE aborda competências profissionais; o CSTA aborda a formação educacional; o COBIT aborda a governança de TI. Cada framework, em sua respectiva dimensão, oferece estruturas consolidadas e amplamente adotadas.

No entanto, a articulação entre esses frameworks ao longo do ciclo de vida da resiliência cibernética constitui um domínio em que perspectivas arquiteturais sistemáticas permanecem comparativamente menos desenvolvidas. A Arquitetura de Resiliência Cibernética Helix se situa precisamente nessa interseção, oferecendo uma perspectiva complementar que organiza a compreensão de como esses frameworks se conectam progressivamente ao longo do ciclo de vida humano e institucional da cibersegurança. As seções subsequentes desenvolvem essa perspectiva, começando pela fundamentação conceitual da arquitetura.

3. Fundamentação Conceitual da Arquitetura Helix

Esta seção apresenta a fundamentação conceitual da Arquitetura de Resiliência Cibernética Helix. Estabelece a necessidade de uma perspectiva arquitetural complementar aos frameworks existentes, define a Helix como tal arquitetura, apresenta seus quatro princípios arquiteturais, identifica o ciclo de vida como seu elemento central e situa a relação conceitual entre a Helix e o ecossistema de frameworks descrito na Seção 2.

3.1 A Necessidade de uma Perspectiva Arquitetural

O campo da cibersegurança desenvolveu profundidade substancial em cada uma de suas dimensões individuais. Controles, competências, sistemas de gestão, padrões educacionais e processos de governança receberam atenção continuada e produziram frameworks consolidados. No entanto, a emergência sustentada da resiliência cibernética ao longo do tempo depende não apenas da profundidade dentro de cada dimensão, mas também da continuidade estrutural que conecta essas dimensões ao longo do ciclo de vida humano e institucional.

Essa continuidade estrutural é observável na prática, mas raramente abordada de forma sistemática em termos conceituais. Indivíduos são formados em contextos educacionais, transitam para ambientes profissionais, consolidam prática operacional e — em alguns casos — assumem responsabilidades de governança ao longo do tempo. Em meio a essas transições, a maturidade desenvolvida em estágios anteriores influencia a maturidade que pode ser sustentada nos estágios subsequentes. Quando essa continuidade é preservada, a resiliência cibernética tende a se consolidar progressivamente. Quando é fragmentada, o valor dos investimentos em qualquer dimensão individual é reduzido.

A observação dessas dinâmicas ao longo de períodos prolongados de prática profissional sugere que a resiliência cibernética se beneficia de uma lente conceitual que torne essa continuidade estrutural observável e passível de estruturação sistemática. Essa lente é arquitetural por natureza: não define novos controles, competências ou processos de governança, mas organiza a compreensão de como esses elementos — já definidos pelos frameworks existentes — se conectam ao longo das trajetórias humanas e institucionais.

3.2 Definição da Arquitetura de Resiliência Cibernética Helix

A Arquitetura de Resiliência Cibernética Helix é definida como uma arquitetura conceitual baseada em ciclo de vida que articula a resiliência cibernética como uma capacidade

em evolução, desenvolvida progressivamente ao longo de três dimensões interdependentes: formação humana, integração operacional e governança. A arquitetura é estruturada em torno de um modelo de maturidade de cinco níveis fundamentado na redução observável do risco, aplicável às três dimensões e conectado por transições críticas que marcam mudanças estruturais na relação do indivíduo com a exposição ao risco cibernético.

Como arquitetura, a Helix enfatiza a coerência estrutural, o desenvolvimento progressivo e o impacto decisório ao longo das trajetórias humanas e institucionais. É explicitamente concebida para ser complementar aos frameworks consolidados, articulando-se com eles em vez de substituí-los. Sua unidade primária de análise é o indivíduo em contexto — isto é, o indivíduo considerado em relação aos ambientes de exposição, prática e responsabilidade em que opera ao longo do ciclo de vida.

3.3 Princípios Arquiteturais

A Arquitetura Helix está fundamentada em quatro princípios arquiteturais que, em conjunto, expressam sua identidade conceitual e orientam sua aplicação.

O primeiro princípio é que a Helix é centrada no humano. A arquitetura é estruturada em torno da trajetória do indivíduo — como os indivíduos são formados, como atuam em ambientes profissionais e como exercem responsabilidade de governança — e não em torno de controles técnicos ou processos organizacionais isolados. Essa orientação centrada no humano reflete a observação de que a resiliência cibernética é, em última instância, sustentada pela maturidade das pessoas que formam, operam e decidem.

O segundo princípio é que a Helix é progressiva. A arquitetura assume que a resiliência cibernética se desenvolve por progressão ao longo do tempo, e não por intervenções discretas ou estáticas. Essa progressão é observável e pode ser estruturada de forma sistemática, o que permite que a maturidade de indivíduos e instituições seja avaliada e apoiada de modo estruturado. O modelo de cinco níveis (desenvolvido na Seção 5) operacionaliza esse princípio, oferecendo um instrumento conceitual para observação da progressão ao longo das curvas da arquitetura.

O terceiro princípio é que a Helix é arquiteturalmente integrada. As três curvas — formativa, operacional e de governança — não são trajetórias independentes; são dimensões interdependentes de uma arquitetura estruturalmente integrada. A maturidade desenvolvida em uma curva influencia a maturidade que pode ser sustentada nas outras. As transições críticas

entre as curvas são elementos arquiteturais que determinam se essa integração é preservada ou fragmentada ao longo do tempo.

O quarto princípio é que a Helix é mensurável. A arquitetura está fundamentada em comportamentos observáveis e avaliáveis sob condições reais. Seu modelo de cinco níveis não é abstrato nem puramente normativo; baseia-se na redução progressiva do risco cibernético, o que oferece fundamento mensurável para sua aplicação. Essa mensurabilidade é central à defensibilidade da arquitetura como referência para observação e avaliação estruturadas.

3.4 O Ciclo de Vida como Elemento Central

O elemento central da Arquitetura Helix é o ciclo de vida da resiliência cibernética. Por ciclo de vida, a arquitetura se refere à trajetória estendida ao longo da qual os indivíduos são formados em ambientes digitais, integram seus comportamentos à prática profissional e — em alguns casos — exercem responsabilidade de governança sobre decisões de cibersegurança. Esse ciclo de vida não é meramente biográfico; é arquitetural. Identifica os momentos estruturais em que a maturidade é desenvolvida, sustentada, transformada ou fragmentada.

A orientação por ciclo de vida distingue a Helix de frameworks que abordam dimensões específicas da cibersegurança de forma isolada. Onde os frameworks existentes abordam controles, competências ou governança em um determinado momento, a Helix aborda como a maturidade em relação a essas dimensões evolui ao longo do tempo. Essa orientação possibilita a observação de fenômenos arquiteturais — continuidade estrutural, transições críticas, maturidade cumulativa — que não são visíveis quando a unidade de análise se restringe a estágios específicos isoladamente.

3.5 Relação Conceitual com os Frameworks

A Arquitetura Helix opera em uma camada conceitual distinta da camada dos frameworks consolidados descritos na Seção 2. Frameworks como o NIST CSF, a ISO/IEC 27001, o NICE Framework, os CSTA Standards e o COBIT abordam o que precisa ser endereçado em suas respectivas dimensões — funções organizacionais, sistemas de gestão, competências profissionais, conteúdo educacional ou processos de governança. A Helix aborda como a maturidade para exercer esses elementos progride ao longo do ciclo de vida humano e institucional.

Essa relação é conceitualmente complementar. Não implica posicionamento hierárquico entre a Helix e os frameworks, nem implica que um substitua o outro. Em vez

disso, a Helix ocupa uma camada arquitetural paralela que se intersecciona com cada framework em pontos específicos de conexão, permitindo que o ecossistema de referências seja observado por uma lente adicional, orientada à continuidade estrutural da resiliência cibernética ao longo do tempo.

3.6 Síntese

A Arquitetura de Resiliência Cibernética Helix, em essência, propõe uma perspectiva estruturada que complementa o ecossistema de frameworks em cibersegurança ao oferecer uma lente arquitetural sobre o ciclo de vida da resiliência cibernética. Fundamentada em quatro princípios arquiteturais, orientada ao indivíduo em contexto e estruturada em torno da interdependência entre formação humana, integração operacional e governança, a Helix busca contribuir para a compreensão da resiliência cibernética como capacidade em evolução, que emerge da continuidade estrutural ao longo do tempo.

As seções subsequentes desenvolvem essa arquitetura em maior detalhe — começando, na Seção 4, pelas três curvas de maturidade que estruturam sua organização interna.

4. As Três Curvas de Maturidade

Esta seção desenvolve as três curvas de maturidade que estruturam a Arquitetura de Resiliência Cibernética Helix. As curvas — formativa, operacional e de governança — constituem a organização interna da arquitetura e representam as três dimensões interdependentes ao longo das quais a resiliência cibernética se desenvolve progressivamente ao longo do tempo. A seção apresenta primeiramente a lógica geral das três curvas, em seguida descreve cada curva individualmente, e conclui com uma discussão de sua interconexão.

4.1 Visão Geral das Três Curvas

As três curvas de maturidade da Arquitetura Helix representam dimensões interdependentes da resiliência cibernética que se desenvolvem ao longo do ciclo de vida humano e institucional. Cada curva corresponde a uma camada específica do ciclo de vida: a curva formativa aborda o desenvolvimento pré-operacional do comportamento e da consciência digital; a curva operacional aborda a integração do comportamento em ambientes profissionais reais; e a curva de governança aborda o alinhamento da resiliência cibernética com a liderança, a responsabilidade executiva e a tomada de decisão estratégica.

As três curvas não são trajetórias independentes. Elas são dimensões interconectadas de uma única arquitetura que organiza a progressão da resiliência cibernética ao longo do tempo. Embora cada curva tenha seu foco específico, todas compartilham uma variável subjacente comum: a maturidade do indivíduo em relação à exposição ao risco cibernético. Essa variável comum confere coerência às três curvas e possibilita a integração arquitetural: a maturidade desenvolvida em uma curva influencia a maturidade que pode ser sustentada nas outras.

A unidade de análise adotada pela Arquitetura Helix é o indivíduo em contexto — o indivíduo considerado em relação aos ambientes de exposição, prática e responsabilidade em que opera. As três curvas descrevem como a maturidade desse indivíduo evolui ao longo de contextos qualitativamente distintos: contextos de formação, contextos de operação e contextos de governança. Cada curva, portanto, não descreve um tipo diferente de indivíduo; descreve o mesmo indivíduo atuando em uma dimensão diferente do ciclo de vida da resiliência cibernética.

4.2 A Curva Formativa

A curva formativa aborda o desenvolvimento pré-operacional do comportamento e da consciência digital. Corresponde à fase do ciclo de vida em que o indivíduo é formado — por meio da exposição educacional, cultural e profissional inicial — em relação à cibersegurança. O foco dessa curva é a maturidade comportamental em relação ao risco digital, abrangendo a aquisição de comportamentos seguros, a construção da consciência digital e o desenvolvimento de padrões reflexivos que preparam o indivíduo para a exposição operacional subsequente.

Na curva formativa, a cibersegurança é abordada tipicamente em contextos de formação educacional ou pré-profissional: educação básica, ensino médio, ensino superior, desenvolvimento inicial de carreira e contextos correlatos. A exposição ao risco cibernético nesses contextos tende a ser mediada, supervisionada e estruturada, permitindo ao indivíduo desenvolver padrões iniciais de comportamento sem enfrentar todas as consequências típicas dos ambientes operacionais. A qualidade da formação nessa curva influencia significativamente a base comportamental que estará disponível quando o indivíduo transitar para ambientes operacionais.

A maturidade desenvolvida na curva formativa, portanto, não é meramente preparatória em sentido temporal; é arquiteturalmente fundacional. Constitui a base comportamental sobre a qual a maturidade operacional e de governança subsequentes podem se desenvolver. Uma base formativa frágil tende a produzir maturidade operacional e de governança frágeis, ainda que competências específicas sejam adquiridas posteriormente. Uma base formativa sólida, ao contrário, oferece a fundação estrutural sobre a qual as curvas subsequentes podem se desenvolver com maior consistência.

4.3 A Curva Operacional

A curva operacional aborda a integração do comportamento digital em ambientes profissionais reais. Corresponde à fase do ciclo de vida em que o indivíduo opera dentro dessa dimensão — exercendo responsabilidade técnica em contextos de cibersegurança, aplicando competências em cenários complexos e sustentando comportamentos sob pressão operacional. O foco dessa curva é a maturidade prática em relação ao risco operacional, abrangendo a consistência de comportamentos em ambientes reais, a integração de competências técnicas com a consciência contextual e a sustentação do desempenho em cenários de complexidade variada.

Na curva operacional, a cibersegurança é abordada em contextos de prática profissional: Centros de Operações de Segurança (Security Operations Centers, SOC), resposta

a incidentes, equipes técnicas em organizações e ambientes operacionais correlatos. A exposição ao risco cibernético nesses contextos é direta, imediata e não mediada: ações e omissões têm consequências concretas sobre sistemas, processos e equipes. O indivíduo opera sob pressão operacional, em cenários frequentemente caracterizados por tempo reduzido para tomada de decisão e pela influência de variáveis ausentes da fase formativa.

A maturidade desenvolvida na curva operacional sustenta, na prática, a resiliência cibernética dos ambientes em que os profissionais atuam. É nessa curva que as competências se tornam prática consistente, que o conhecimento técnico se traduz em capacidade operacional e que os padrões comportamentais desenvolvidos na curva formativa são testados sob condições reais. A curva operacional é, portanto, a dimensão em que o profissional efetivamente contribui para a manutenção diária da cibersegurança em ambientes compartilhados.

4.4 A Curva de Governança

A curva de governança aborda o alinhamento da resiliência cibernética com a liderança, a responsabilidade executiva e a tomada de decisão estratégica. Corresponde à fase do ciclo de vida em que o indivíduo exerce papel de influência estratégica sobre o risco cibernético — seja por meio da governança direta da cibersegurança, seja por decisões executivas que impactam a postura de cibersegurança das organizações, seja por meio da liderança em contextos cujas decisões moldam as condições de resiliência em ecossistemas mais amplos. O foco dessa curva é a maturidade decisória em relação ao risco estratégico, abrangendo a capacidade de situar o risco cibernético no processo decisório estratégico, articular a cibersegurança com objetivos institucionais mais amplos e estruturar mecanismos de prestação de contas que sustentem a resiliência ao longo do tempo.

Na curva de governança, a cibersegurança é abordada em contextos de responsabilidade executiva e estratégica: posições de Chief Information Security Officer (CISO), comitês de risco, conselhos de administração e estruturas de governança correlatas. A exposição ao risco cibernético nesses contextos é sistêmica: as decisões tomadas nessa dimensão influenciam a postura de cibersegurança de organizações inteiras e, em alguns casos, de ecossistemas mais amplos. O impacto da maturidade de governança se estende além do indivíduo que a exerce, moldando as condições sob as quais os profissionais operam e os indivíduos são formados.

A maturidade desenvolvida na curva de governança não é adquirida apenas pela posição formal. Requer a articulação da experiência operacional acumulada, a capacidade de situar a

cibersegurança em contextos estratégicos mais amplos e o desenvolvimento de uma visão sistêmica do risco cibernético. Um tomador de decisão com maturidade de governança consolidada contribui para estruturar condições de resiliência que se estendem além de sua prática individual, influenciando o ambiente operacional em que os profissionais atuam e o ambiente formativo em que futuros indivíduos serão formados.

4.5 Interconexão entre as Três Curvas

As três curvas da Arquitetura Helix estão estruturalmente interconectadas. A maturidade desenvolvida em uma curva influencia, de modos específicos, a maturidade que pode ser sustentada nas outras. Essa interconexão ocorre em múltiplas direções.

Na direção ascendente, a curva formativa estabelece a base comportamental sobre a qual a curva operacional é construída, a qual, por sua vez, oferece a base experiencial sobre a qual a curva de governança se consolida. Um indivíduo com maturidade formativa frágil tende a enfrentar maiores dificuldades para consolidar maturidade operacional, e uma maturidade operacional consolidada é tipicamente requerida para o desenvolvimento de uma maturidade de governança robusta. Essa direção ascendente representa o desenvolvimento arquitetural progressivo da resiliência cibernética ao longo do ciclo de vida.

Na direção descendente, a maturidade na curva de governança molda as condições sob as quais os indivíduos operam na curva operacional e sob as quais são formados na curva formativa. Decisões de governança definem recursos, prioridades estratégicas, culturas organizacionais e estruturas institucionais que influenciam diretamente os ambientes operacionais e formativos. Uma maturidade de governança consolidada, portanto, estende seus efeitos a toda a arquitetura, enquanto uma maturidade de governança frágil pode comprometer a resiliência dos ambientes que ela influencia.

As três curvas, em sua interconexão estrutural, constituem a organização interna da Arquitetura de Resiliência Cibernética Helix. A observação dessa interconexão, e das transições críticas que conectam as curvas, constitui uma das contribuições arquiteturais centrais deste artigo. A Seção 5 apresenta o modelo de maturidade de cinco níveis aplicável às três curvas, e a Seção 6 desenvolve em detalhe as transições críticas entre elas.

5. O Modelo de Maturidade em Cinco Níveis

Esta seção apresenta o modelo de maturidade em cinco níveis que opera ao longo das três curvas da Arquitetura de Resiliência Cibernética Helix. O modelo oferece um meio estruturado de descrever a progressão dentro de cada curva, fundamentado na redução observável do risco sob condições reais. A seção apresenta primeiramente a lógica geral do modelo, em seguida descreve cada um dos cinco níveis individualmente, seguido pela lógica de mensuração baseada em risco que sustenta o modelo, pela metodologia de avaliação proposta para sua aplicação, e, finalmente, por sua aplicação ao longo das três curvas.

5.1 Visão Geral do Modelo

O modelo de cinco níveis da Arquitetura Helix descreve a progressão da maturidade dentro de cada uma das três curvas. Cada nível representa um estágio qualitativamente distinto do desenvolvimento do indivíduo em relação à exposição ao risco cibernético dentro da curva considerada. Os níveis são progressivos — isto é, cada nível subsequente pressupõe, em essência, a consolidação do nível anterior — mas não seguem uma sequência linear rígida. Trajetórias individuais podem apresentar variações, regressões e platôs, refletindo a complexidade do desenvolvimento real em relação à cibersegurança.

Os cinco níveis são: Exposição Fundacional (Nível 1), Formação Comportamental (Nível 2), Consistência Comportamental (Nível 3), Integração Operacional (Nível 4) e Liderança Arquitetural (Nível 5). Esses níveis são aplicáveis a cada uma das três curvas, embora sua manifestação específica varie conforme a curva considerada. O modelo, portanto, é transversal à arquitetura: os mesmos cinco níveis descrevem a progressão na curva formativa, na curva operacional e na curva de governança.

A transversalidade do modelo não implica uniformidade de manifestação. Cada nível assume características específicas em cada curva, refletindo as diferenças qualitativas entre os contextos formativos, operacionais e de governança. A Seção 5.5 desenvolve essas manifestações específicas, após a apresentação dos cinco níveis em sua forma geral.

5.2 Os Cinco Níveis

As subseções seguintes descrevem os cinco níveis da Arquitetura Helix em sua forma geral. As manifestações específicas ao longo das três curvas são abordadas posteriormente, na Seção 5.5.

5.2.1 Nível 1 — Exposição Fundacional

O Nível 1 representa o estágio inicial do desenvolvimento do indivíduo em relação ao risco cibernético. Nesse nível, o indivíduo está exposto a ambientes digitais sem ter consolidado padrões específicos de comportamento seguro na curva considerada. A exposição é essencialmente passiva: o indivíduo experiencia situações digitais sem ainda dispor da fundação comportamental, operacional ou decisória necessária para responder a elas com consistência.

O Nível 1 pode caracterizar indivíduos em estágios iniciais da formação digital, profissionais em integração inicial em novos ambientes operacionais ou tomadores de decisão com engajamento recente em governança de cibersegurança — especialmente quando ainda não dispõem de padrões transferíveis suficientemente consolidados para esse novo ambiente. Nesse nível, o risco de a conduta do indivíduo produzir vulnerabilidades de cibersegurança é comparativamente alto, refletindo a ausência de padrões específicos consolidados para a curva em questão.

5.2.2 Nível 2 — Formação Comportamental

O Nível 2 representa o estágio em que o indivíduo começa a desenvolver padrões iniciais de comportamento apropriados à curva considerada. Nesse nível, o indivíduo já foi exposto a conceitos e práticas de cibersegurança e começa a incorporá-los à sua conduta — ainda que de modo inconsistente, com variações conforme o contexto, a pressão e a complexidade do cenário.

A formação comportamental se caracteriza pela emergência da consciência em relação ao risco digital, pela adoção inicial de práticas seguras e pelo início do desenvolvimento de padrões reflexivos. A conduta do indivíduo nesse estágio reflete uma compreensão da importância da cibersegurança, mas a aplicação dessa compreensão ainda depende, em alguma medida, de lembretes explícitos, suporte direto ou cenários de complexidade reduzida. O risco de eventos adversos ocorrerem é menor do que no Nível 1, mas ainda não suficientemente reduzido para caracterizar resiliência robusta.

5.2.3 Nível 3 — Consistência Comportamental

O Nível 3 representa a consolidação dos padrões comportamentais desenvolvidos no nível anterior. Nesse nível, o indivíduo apresenta consistência na aplicação de comportamentos seguros em contextos variados, incluindo aqueles de pressão e complexidade moderadas. Os

comportamentos seguros foram internalizados como prática padrão, não dependendo mais de lembretes explícitos ou de suporte estruturado para sua manutenção.

A consistência comportamental se manifesta na sustentação de comportamentos seguros sob condições reais, na autonomia progressiva do indivíduo em relação a decisões de cibersegurança dentro de seu escopo de atuação e na variabilidade reduzida de respostas comportamentais em cenários similares. O risco de eventos adversos ocorrerem nesse nível é significativamente reduzido, refletindo a consolidação de padrões que sustentam a resiliência do indivíduo na curva considerada.

5.2.4 Nível 4 — Integração Operacional

O Nível 4 representa o estágio em que o indivíduo integra seus comportamentos consolidados ao contexto operacional mais amplo em que atua. Nesse nível, o indivíduo não apenas mantém a consistência comportamental, mas contribui para a resiliência do ambiente como um todo, articulando sua prática com a de outros indivíduos, com processos organizacionais e com os requisitos específicos do contexto em que opera.

A integração operacional se caracteriza pela compreensão sistêmica do ambiente, pela articulação entre prática individual e objetivos organizacionais e pela capacidade de sustentar a resiliência em cenários complexos e mutáveis. O indivíduo nesse nível exerce autonomia prática e contribui ativamente para a postura mais ampla de cibersegurança do ambiente em que atua. O risco de eventos adversos no escopo de sua prática é substancialmente reduzido, refletindo não apenas a consistência individual, mas também a integração efetiva ao contexto operacional.

5.2.5 Nível 5 — Liderança Arquitetural

O Nível 5 representa o estágio mais avançado da Arquitetura Helix. Nesse nível, o indivíduo exerce papel de liderança arquitetural em relação à resiliência cibernética: estrutura as condições sob as quais outros indivíduos operam, influencia os contextos de tomada de decisão estratégica sobre cibersegurança e contribui para a configuração sistêmica da resiliência ao longo dos ambientes em que atua.

A liderança arquitetural não corresponde simplesmente à posição formal de liderança. Representa um nível qualitativo de maturidade em que o indivíduo, independentemente de sua posição formal, exerce impacto estrutural sobre a postura de cibersegurança do ambiente considerado. Nesse nível, a influência do indivíduo se estende à estruturação dos ambientes em

que opera, à formação de outros indivíduos e à articulação entre objetivos estratégicos e realidades operacionais em cibersegurança. O risco de eventos adversos sob seu escopo de influência é significativamente reduzido, refletindo o impacto de sua liderança arquitetural sobre as condições sistêmicas de resiliência.

5.3 Lógica de Mensuração Baseada em Risco

A lógica central de mensuração dos cinco níveis da Arquitetura Helix está fundamentada na redução observável do risco. Cada nível corresponde a um estágio progressivo de redução do risco cibernético que emerge da conduta do indivíduo na curva considerada. Essa lógica é operacionalizada por meio da relação entre probabilidade e impacto de eventos adversos, segundo a fórmula $\text{Risk Score} = \text{Likelihood} \times \text{Impact}$ (Pontuação de Risco = Probabilidade \times Impacto), consistente com a abordagem orientada a riscos adotada por frameworks como a ISO/IEC 27001 e o NIST CSF.

Em cada nível, a redução do risco se manifesta de modos específicos. Em níveis inferiores, a redução é predominantemente local e individual, refletindo a consolidação de padrões comportamentais específicos. Em níveis intermediários, a redução se torna mais consistente e integrada ao contexto operacional. Em níveis superiores, a redução adquire impacto sistêmico, refletindo a influência da liderança arquitetural sobre as condições estruturais de resiliência.

Essa lógica de mensuração fundamentada na redução observável do risco distingue o modelo Helix de modelos de maturidade puramente normativos. Em vez de prescrever comportamentos como desejáveis em si mesmos, o modelo Helix conecta a observação dos comportamentos ao impacto específico que eles produzem sobre a redução do risco cibernético. Essa fundamentação confere defensibilidade empírica à classificação dos níveis de maturidade e oferece base objetiva para sua avaliação ao longo das três curvas da arquitetura.

5.4 Metodologia de Avaliação

A metodologia de avaliação proposta para a Arquitetura Helix combina três abordagens complementares, concebidas para possibilitar uma classificação defensável da maturidade ao longo dos cinco níveis. Essa metodologia é transversal às três curvas da arquitetura e pode ser adaptada a contextos específicos de aplicação.

A primeira abordagem é a avaliação da compreensão conceitual, que avalia se o indivíduo possui o fundamento conceitual específico requerido para a curva e o nível

considerados. Essa avaliação pode incluir instrumentos estruturados de conhecimento, entrevistas dirigidas ou discussões contextualizadas. Seu objetivo é identificar a presença ou ausência conceitual necessária à prática consistente no nível avaliado.

A segunda abordagem é a avaliação baseada em cenários, que avalia o comportamento do indivíduo em situações construídas para reproduzir, de modo controlado, as condições específicas da curva considerada. Essa avaliação pode incluir exercícios, simulações ou estudos de caso, e permite a observação de comportamentos aplicados sob condições que se aproximam da prática real. Seu objetivo é verificar se o fundamento conceitual do indivíduo se traduz em comportamento apropriado sob condições de pressão contextual.

A terceira abordagem é a observação longitudinal, que avalia a conduta do indivíduo ao longo do tempo em contextos de prática continuada. Essa avaliação requer protocolos estruturados de observação, indicadores comportamentais e períodos de acompanhamento suficientes para capturar a consistência sob condições reais. Seu objetivo é confirmar se os padrões evidenciados em instrumentos de avaliação conceitual e baseada em cenários se sustentam na prática continuada — condição essencial para a caracterização como maturidade consolidada.

5.5 Aplicação ao Longo das Três Curvas

Os cinco níveis da Arquitetura Helix se aplicam às três curvas: formativa, operacional e de governança. A lógica geral dos níveis é preservada nas três curvas, mas a manifestação específica de cada nível varia conforme as características qualitativas da curva considerada.

Na curva formativa, os cinco níveis descrevem a progressão da maturidade comportamental em relação ao risco digital, desde a exposição fundacional inicial até uma liderança arquitetural emergente em contextos formativos. O profissional de Nível 5 na curva formativa tipicamente assume influência formativa sobre outros indivíduos: contribui, por meio do ensino, da criação de conteúdo, da estruturação pedagógica ou de vetores análogos, para a formação de indivíduos ao longo da mesma curva, estruturando as condições formativas de outros.

Na curva operacional, os cinco níveis descrevem a progressão da maturidade prática em relação ao risco operacional, desde a integração inicial do indivíduo em um ambiente operacional específico até a liderança arquitetural em contextos operacionais. O profissional de Nível 5 na curva operacional exerce impacto estrutural sobre a resiliência dos ambientes

operacionais em que atua, influenciando práticas, processos, culturas organizacionais e a articulação entre equipes operacionais.

Na curva de governança, os cinco níveis descrevem a progressão da maturidade decisória em relação ao risco estratégico, desde o engajamento inicial em decisões de cibersegurança até a liderança arquitetural em contextos de governança. O profissional de Nível 5 na curva de governança exerce impacto sistêmico sobre a postura de cibersegurança, influenciando a estruturação das condições organizacionais e institucionais de resiliência cibernética e articulando decisões de governança com as realidades operacionais e formativas.

A transversalidade dos cinco níveis é, portanto, um elemento arquitetural central da Helix. Possibilita a comparação da progressão entre diferentes curvas, a articulação de avaliações entre dimensões distintas do ciclo de vida e a construção de uma visão integrada da maturidade do indivíduo em cibersegurança ao longo da arquitetura.

6. Transições Críticas ao Longo do Ciclo de Vida

A seção anterior apresentou o modelo de maturidade em cinco níveis aplicável às três curvas da Arquitetura de Resiliência Cibernética Helix. Esta seção desenvolve um elemento arquitetural mencionado em seções anteriores e aprofundado aqui de modo dedicado: as transições críticas entre as curvas de maturidade. Essas transições constituem pontos de descontinuidade estrutural nos quais a progressão da resiliência cibernética pode ser consolidada ou fragmentada, dependendo das condições sob as quais ocorrem.

6.1 O Conceito de Transições Críticas

As três curvas de maturidade que constituem a Arquitetura Helix — formativa, operacional e de governança — estão estruturalmente interconectadas, conforme estabelecido na Seção 4. Entretanto, a progressão de uma curva para outra não ocorre de modo contínuo e linear. Existem pontos específicos da trajetória em que o indivíduo transita entre contextos qualitativamente distintos de exposição e responsabilidade, e esses pontos exigem reconfiguração dos padrões de maturidade previamente consolidados.

Esses pontos são denominados transições críticas, em que o adjetivo "crítica" denota seu significado arquitetural, e não a severidade do risco. São momentos em que a continuidade da resiliência cibernética ao longo do ciclo de vida depende de adaptação estrutural, e não apenas de acúmulo progressivo. Uma transição crítica inadequadamente apoiada pode comprometer a maturidade desenvolvida em contextos anteriores; uma transição adequadamente apoiada, ao contrário, consolida e expande essa maturidade para novos domínios de atuação.

Duas transições críticas são particularmente relevantes para a arquitetura Helix: a transição da curva formativa para a curva operacional e a transição da curva operacional para a curva de governança. Ambas envolvem mudanças significativas no tipo de exposição enfrentada, no escopo de responsabilidade exercida e nas manifestações observáveis de maturidade. Esta seção desenvolve cada uma dessas transições, seguida de uma reflexão sobre as implicações arquiteturais mais amplas que elas revelam.

Antes de abordar cada transição especificamente, é útil reconhecer uma característica comum a ambas: em cada caso, a transição não é meramente cronológica ou contextual; é arquitetural. O indivíduo que transita entre curvas não simplesmente muda de ambiente — passa a operar sob lógicas qualitativamente distintas de exposição e responsabilidade, que

exigem reconfiguração dos padrões comportamentais, das competências técnicas e das capacidades decisórias previamente consolidadas.

6.2 Transição da Curva Formativa para a Curva Operacional

A primeira transição crítica ocorre quando o indivíduo deixa um contexto predominantemente formativo — em que a exposição é estruturada, supervisionada e orientada ao desenvolvimento comportamental — e ingressa em um contexto operacional, em que a exposição é real, as consequências são concretas e a responsabilidade técnica passa a ser exercida sem mediação direta dos mecanismos de supervisão característicos da fase formativa.

Essa transição envolve uma mudança substantiva na natureza da exposição. Na curva formativa, os cenários de risco são frequentemente controlados, simulados ou apresentados em contextos educacionais nos quais os erros podem ser corrigidos sem amplas consequências operacionais. Na curva operacional, em contraste, os cenários de risco ocorrem em ambientes reais, nos quais ações ou omissões têm efeitos diretos sobre sistemas, processos e equipes. O indivíduo, portanto, passa de uma relação mediada com o risco para uma relação direta com ele.

A passagem entre essas duas lógicas de exposição requer reconfiguração comportamental significativa. Comportamentos seguros desenvolvidos em contexto formativo precisam ser sustentados sob pressão operacional, em cenários complexos, frequentemente com tempo reduzido para tomada de decisão e sob a influência de variáveis que não estavam presentes durante a formação. Essa sustentação não é automática: depende da consolidação prévia de padrões comportamentais na curva formativa (particularmente no Nível 3 — Consistência Comportamental) e da existência de condições operacionais que apoiem a integração progressiva do indivíduo ao novo contexto.

Quando essa transição ocorre de modo adequadamente apoiado, observa-se continuidade estrutural entre as curvas: o indivíduo preserva os padrões comportamentais desenvolvidos na fase formativa e os expande em complexidade técnica e contextual ao longo da curva operacional. Quando a transição ocorre sem apoio adequado — seja pela ausência de consolidação prévia na curva formativa, seja pela ausência de condições operacionais que permitam integração progressiva —, observa-se descontinuidade: comportamentos seguros desenvolvidos em contexto formativo não se traduzem em prática profissional consistente, e a maturidade operacional precisa ser reconstruída sob pressão, o que tende a produzir resultados instáveis.

A transição da curva formativa para a curva operacional é, portanto, um ponto arquitetural de alta importância. Define se os investimentos realizados na fase formativa serão convertidos em capacidade operacional real ou se se dissiparão durante a entrada do indivíduo em ambientes profissionais. A qualidade dessa transição é, em grande medida, uma responsabilidade compartilhada entre as condições formativas anteriores, as condições operacionais receptoras e as estruturas de apoio que conectam as duas dimensões.

6.3 Transição da Curva Operacional para a Curva de Governança

A segunda transição crítica ocorre quando o indivíduo, tendo consolidado maturidade operacional em contextos de responsabilidade técnica, passa a exercer papéis em que suas decisões influenciam sistematicamente a resiliência cibernética de organizações, instituições ou ecossistemas mais amplos. Trata-se da transição da execução operacional consistente para a tomada de decisão estratégica estruturada.

Essa transição envolve uma mudança qualitativa no escopo e na natureza da responsabilidade exercida. Na curva operacional, a responsabilidade do indivíduo se manifesta predominantemente por meio da execução técnica consistente e da contribuição direta para a redução de risco em ambientes compartilhados. Na curva de governança, a responsabilidade se expande à estruturação das condições sob as quais essa execução ocorre — envolvendo alocação de recursos, alinhamento estratégico, definição de prioridades institucionais e articulação entre cibersegurança e objetivos organizacionais mais amplos.

A passagem entre essas duas lógicas de responsabilidade requer reconfiguração das capacidades decisórias e da perspectiva temporal do indivíduo. Competências técnicas e comportamentos consistentes desenvolvidos na curva operacional permanecem relevantes, mas deixam de ser, por si sós, suficientes para sustentar a maturidade na curva de governança. A tomada de decisão estratégica em cibersegurança requer, adicionalmente, uma visão sistêmica do risco, a capacidade de articular considerações de cibersegurança com diversas dimensões institucionais e a compreensão das implicações de longo prazo das decisões tomadas.

Quando essa transição ocorre de modo adequadamente apoiado, a experiência operacional anterior é convertida em fundação para a tomada de decisão estratégica informada. O tomador de decisão que transitou adequadamente da curva operacional para a curva de governança traz a suas decisões uma compreensão concreta dos contextos sobre os quais decide, o que tende a produzir alinhamento mais efetivo entre decisões de governança e realidades operacionais. Quando a transição ocorre sem apoio adequado — seja pelo

deslocamento prematuro do indivíduo a papéis decisórios sem consolidação operacional anterior, seja pela ausência de estruturas que apoiem o desenvolvimento da visão sistêmica requerida pela curva de governança —, observa-se desalinhamento entre decisão e execução: decisões estratégicas podem não refletir adequadamente as realidades operacionais que pretendem endereçar, e a prática operacional pode não ser efetivamente sustentada por decisões de governança.

A transição da curva operacional para a curva de governança é, portanto, outro ponto arquitetural crítico. Define se a experiência acumulada em ambientes operacionais será convertida em tomada de decisão estratégica bem fundamentada ou se será dissipada na passagem a contextos decisórios. Tal como na transição anterior, a qualidade dessa passagem depende tanto da consolidação prévia na curva operacional quanto da existência de condições, na curva de governança, que apoiem a integração progressiva do indivíduo a sua nova responsabilidade.

6.4 Implicações Arquiteturais das Transições

As duas transições críticas descritas nas subseções anteriores revelam propriedades arquiteturais mais amplas da Helix, que merecem ênfase para uma compreensão completa do modelo.

A primeira implicação é que a continuidade da resiliência cibernética ao longo do ciclo de vida não é um subproduto automático da passagem do tempo ou do acúmulo de experiência. Depende, em pontos específicos do ciclo, de condições estruturais que apoiem a reconfiguração da maturidade em contextos qualitativamente novos. Essa observação reforça o princípio arquitetural de que a resiliência cibernética é progressiva (Seção 3.3), mas também explicita que a progressão envolve descontinuidades que precisam ser intencionalmente apoiadas.

A segunda implicação é que os investimentos realizados em cada curva não são autocontidos: seu valor para a resiliência cibernética ao longo do ciclo de vida depende, em parte, da qualidade das transições que conectam essa curva às outras. Investimentos robustos na curva formativa podem produzir efeitos limitados se a transição para a curva operacional não for apoiada; de modo análogo, experiência operacional consolidada pode produzir decisões de governança desconectadas se a transição para a curva de governança ocorrer sem condições adequadas. A continuidade estrutural, portanto, emerge não apenas do desenvolvimento dentro de cada curva, mas da qualidade das pontes arquiteturais entre elas.

A terceira implicação é que as transições críticas constituem pontos naturais de atenção para iniciativas de cibersegurança que buscam sustentar a resiliência ao longo do ciclo de vida. Tais iniciativas podem reconhecer e abordar as transições como elementos arquiteturais específicos — distintos do desenvolvimento dentro de cada curva — e estruturar condições que apoiem a reconfiguração da maturidade nesses pontos. Essa abordagem é complementar, e não substitutiva, em relação aos esforços focados no desenvolvimento dentro das curvas.

A quarta implicação diz respeito à reciprocidade entre curvas, mencionada na Seção 4.5. As transições críticas não são apenas pontos de passagem ascendente ao longo do ciclo de vida; são também pontos em que a influência recíproca entre curvas se manifesta com particular intensidade. Decisões de governança estruturam as condições sob as quais ocorre a transição da curva operacional para a curva de governança, assim como definem em grande medida as condições sob as quais ocorre a transição da curva formativa para a curva operacional. A prática operacional consistente, por sua vez, influencia o modo como decisões de governança reconhecem e apoiam as transições. Essa reciprocidade estrutural reforça o caráter arquitetural — e não linear — da Helix.

6.5 Síntese das Transições Críticas

As transições críticas descritas nesta seção são, em essência, pontos arquiteturais nos quais a continuidade da resiliência cibernética é particularmente sensível às condições estruturais que apoiam ou restringem a progressão do indivíduo entre contextos qualitativamente distintos de exposição e responsabilidade.

A transição da curva formativa para a curva operacional define em que medida o comportamento digital desenvolvido em contextos pré-operacionais se traduz em prática profissional consistente. A transição da curva operacional para a curva de governança define em que medida a experiência acumulada em contextos operacionais se converte em tomada de decisão estratégica informada. Ambas são, simultaneamente, momentos de potencial vulnerabilidade — em que a continuidade pode se fragmentar — e momentos de potencial consolidação — em que a maturidade desenvolvida em uma dimensão pode se expandir para outra.

Reconhecer essas transições como elementos arquiteturais específicos é uma das contribuições da Helix para a compreensão da resiliência cibernética ao longo do ciclo de vida. Essa contribuição complementa a compreensão estrutural oferecida pelas três curvas (Seção 4) e pelo modelo de maturidade em cinco níveis (Seção 5), oferecendo uma lente adicional que

ênfatiza a importância das pontes arquiteturais entre as curvas, e não apenas o desenvolvimento dentro delas.

A próxima seção apresenta domínios de aplicação em que a Helix — incluindo seu modelo de curvas, seus cinco níveis de maturidade e sua perspectiva sobre as transições críticas — pode ser utilizada de modo complementar a iniciativas e frameworks existentes.

7. Domínios de Aplicação

A Arquitetura de Resiliência Cibernética Helix, dada sua natureza arquitetural e sua orientação por ciclo de vida, pode ser utilizada como perspectiva complementar em diferentes domínios em que a resiliência cibernética constitui elemento relevante. Esta seção apresenta uma descrição desses domínios de aplicação, focalizando como a Helix pode oferecer uma lente arquitetural que complementa iniciativas e frameworks existentes em cada contexto. O propósito desta seção não é prescrever formas específicas de adoção, mas ilustrar como a lógica arquitetural da Helix pode ser observada em domínios diversos.

7.1 Visão Geral dos Domínios de Aplicação

Os domínios de aplicação da Helix correspondem a contextos em que a resiliência cibernética evolui ao longo do tempo por meio das dimensões formativa, operacional e de governança. Em cada um desses domínios, frameworks específicos já oferecem referências consolidadas para controles, competências, práticas educacionais ou processos de governança. A Helix, como perspectiva complementar, pode ser aplicada como lente arquitetural que organiza a compreensão de como essas referências existentes se conectam progressivamente ao longo da trajetória humana e institucional no domínio considerado.

A aplicação da Helix em cada domínio assume formas distintas, refletindo as características específicas do contexto. Em ambientes educacionais, a ênfase recai predominantemente sobre a curva formativa e a transição da curva formativa para a operacional. Em contextos de desenvolvimento profissional, a ênfase se desloca para a curva operacional e para a consolidação da maturidade em ambientes técnicos. Em domínios de infraestrutura crítica, a aplicação envolve a articulação entre as três curvas, dada a complexidade e o impacto sistêmico típicos desses ambientes. Em contextos de governança corporativa e liderança estratégica, a ênfase recai sobre a curva de governança e sobre a transição da curva operacional para a curva de governança.

Esta seção apresenta quatro domínios representativos — ambientes educacionais, contextos de desenvolvimento profissional, proteção de infraestrutura crítica e governança corporativa — seguidos de uma reflexão sobre a integração entre os domínios. Os domínios descritos não constituem lista exaustiva, mas ilustram a diversidade de contextos em que a perspectiva arquitetural da Helix pode oferecer valor complementar.

7.2 Ambientes Educacionais

Os ambientes educacionais — da educação básica ao ensino superior — constituem o domínio em que a curva formativa da Helix se manifesta de modo mais evidente. Nesses contextos, a resiliência cibernética começa a se desenvolver pelo contato inicial dos estudantes com ambientes digitais, pela construção de padrões comportamentais seguros e pela emergência da consciência sobre exposição e responsabilidade digital.

Frameworks como os CSTA K-12 Computer Science Standards oferecem referências consolidadas para o desenvolvimento de competências digitais e para a inclusão de tópicos de cibersegurança na educação básica. A Helix pode complementar esses frameworks ao oferecer uma lente arquitetural que organiza a compreensão de como as competências desenvolvidas durante a fase formativa se conectam progressivamente aos estágios subsequentes da trajetória do estudante. Essa conexão é particularmente relevante porque a efetividade dos esforços formativos depende, em parte, de como esses esforços se articulam às fases subsequentes do desenvolvimento.

A aplicação da Helix em ambientes educacionais pode oferecer contribuições específicas em três dimensões. Primeiro, permite que a progressão dos estudantes ao longo dos cinco níveis de maturidade, dentro da curva formativa, seja observada por meio de indicadores comportamentais, e não apenas de avaliações teóricas. Segundo, oferece uma perspectiva estruturada sobre a transição da curva formativa para a operacional — particularmente relevante para iniciativas educacionais voltadas à formação inicial em cibersegurança e em áreas correlatas de tecnologia. Terceiro, contribui para a articulação entre programas educacionais em diferentes níveis, favorecendo a continuidade estrutural da resiliência cibernética ao longo da trajetória do estudante.

Em contextos educacionais, a perspectiva arquitetural da Helix não substitui abordagens pedagógicas nem redefine competências curriculares. Seu papel é oferecer uma lente adicional que facilita a compreensão de como a formação digital se integra ao ciclo de vida mais amplo da resiliência cibernética, sustentando a continuidade entre o que é desenvolvido no ambiente educacional e o que será exercido em ambientes profissionais e, eventualmente, em contextos de governança.

7.3 Contextos de Desenvolvimento Profissional

Os contextos de desenvolvimento profissional em cibersegurança — incluindo Centros de Operações de Segurança (SOCs), Centros de Operações de Rede (NOCs), equipes de resposta a incidentes e áreas técnicas em organizações de diferentes setores — constituem o domínio em que a curva operacional da Helix se manifesta de modo mais intenso. Nesses ambientes, profissionais exercem responsabilidade técnica em cenários de complexidade variada, nos quais a consistência comportamental, a capacidade de resposta em tempo real e a integração entre competência técnica e contexto operacional são elementos centrais da resiliência cibernética.

Frameworks como o NICE Workforce Framework for Cybersecurity oferecem referências consolidadas para competências profissionais, papéis de trabalho e trilhas de desenvolvimento em cibersegurança. A Helix pode complementar esses frameworks ao oferecer uma lente arquitetural que organiza a compreensão de como a maturidade necessária ao exercício das competências profissionais evolui ao longo do tempo, desde a integração inicial do profissional em ambientes operacionais até a consolidação da autonomia e da consistência técnica em cenários complexos.

A aplicação da Helix em contextos de desenvolvimento profissional pode oferecer contribuições específicas em três dimensões. Primeiro, permite que a progressão dos profissionais ao longo dos cinco níveis de maturidade, dentro da curva operacional, seja observada por meio de indicadores comportamentais e operacionais sustentados ao longo do tempo. Segundo, oferece uma perspectiva estruturada sobre a transição da curva formativa para a operacional — particularmente relevante para programas que integram novos profissionais, nos quais a qualidade dessa transição influencia diretamente os resultados operacionais subsequentes. Terceiro, contribui para a compreensão de até que ponto a experiência operacional acumulada prepara o profissional para a eventual transição à curva de governança.

Em contextos profissionais, a perspectiva arquitetural da Helix não substitui programas de treinamento, trilhas de carreira ou avaliações de desempenho. Seu papel é oferecer uma lente adicional que facilita a compreensão de como a maturidade técnica se desenvolve progressivamente e como essa progressão se conecta aos estágios anteriores e posteriores do ciclo de vida profissional em cibersegurança.

7.4 Proteção de Infraestrutura Crítica

A proteção de infraestrutura crítica — incluindo setores como energia, telecomunicações, saúde, serviços financeiros, transporte e operações industriais — constitui

domínio de aplicação particularmente relevante para a Helix, dada a articulação intrínseca entre as dimensões formativa, operacional e de governança que caracteriza esses contextos. Nesses ambientes, a resiliência cibernética não depende apenas de controles técnicos específicos; depende também da continuidade estrutural entre o desenvolvimento dos profissionais que operam sistemas críticos, a prática operacional consistente nesses sistemas e as decisões de governança que sustentam a resiliência em escala sistêmica.

Frameworks como o NIST Cybersecurity Framework e a ISO/IEC 27001 oferecem referências consolidadas para a estruturação de funções de cibersegurança e sistemas de gestão aplicáveis a contextos de infraestrutura crítica. A Helix pode complementar esses frameworks ao oferecer uma lente arquitetural que organiza a compreensão de como a maturidade humana e institucional necessária à sustentação dessas referências evolui progressivamente ao longo do tempo em ambientes de infraestrutura crítica.

A aplicação da Helix em contextos de infraestrutura crítica pode oferecer contribuições específicas em quatro dimensões. Primeiro, permite observar como comportamentos desenvolvidos em contextos formativos se sustentam — ou se fragmentam — quando profissionais são integrados aos ambientes operacionais de alta complexidade típicos de infraestruturas críticas. Segundo, oferece perspectiva sobre a qualidade das transições entre as curvas em contextos nos quais o impacto operacional das discontinuidades é particularmente significativo. Terceiro, contribui para a articulação entre decisões de governança em cibersegurança e as realidades operacionais específicas de setores críticos, favorecendo o alinhamento entre as camadas estratégica e técnica. Quarto, possibilita observação longitudinal da maturidade em cibersegurança em contextos nos quais a continuidade estrutural é condição essencial para a sustentação da resiliência ao longo do tempo.

Em domínios de infraestrutura crítica, a perspectiva arquitetural da Helix não substitui frameworks regulatórios, padrões técnicos específicos ou práticas setoriais consolidadas de proteção. Seu papel é oferecer uma lente adicional que facilita a compreensão sistêmica da resiliência cibernética em ambientes nos quais a continuidade estrutural entre as dimensões humana, operacional e estratégica é especialmente significativa.

7.5 Governança Corporativa e Liderança Estratégica

Os contextos de governança corporativa e liderança estratégica em cibersegurança — incluindo posições como Chief Information Security Officer (CISO), diretorias de risco tecnológico, comitês de governança e conselhos de administração — constituem o domínio em

que a curva de governança da Helix se manifesta de modo mais direto. Nesses contextos, decisões estratégicas influenciam sistematicamente a postura de cibersegurança de organizações e ecossistemas, e a qualidade dessas decisões depende, em grande medida, da maturidade dos tomadores de decisão para situar o risco cibernético no processo decisório estratégico.

Frameworks como o ISACA COBIT oferecem referências consolidadas para a integração entre governança de TI e objetivos corporativos, incluindo dimensões específicas relacionadas à cibersegurança. A Helix pode complementar esses frameworks ao oferecer uma lente arquitetural que organiza a compreensão de como a maturidade decisória em cibersegurança evolui progressivamente ao longo da trajetória do tomador de decisão, conectando-se a experiências anteriores em contextos operacionais e formativos.

A aplicação da Helix em contextos de governança corporativa pode oferecer contribuições específicas em três dimensões. Primeiro, permite observar como a experiência operacional acumulada se converte — ou deixa de se converter — em tomada de decisão estratégica informada, por meio da observação da qualidade da transição da curva operacional para a de governança. Segundo, oferece perspectiva sobre como decisões de governança em cibersegurança se articulam com as curvas anteriores, reforçando ou enfraquecendo as condições sob as quais profissionais operam e indivíduos são formados. Terceiro, contribui para a compreensão do impacto sistêmico das decisões executivas sobre a resiliência cibernética de organizações e ecossistemas, ampliando o escopo de análises frequentemente focadas em indicadores operacionais discretos.

Em contextos de governança, a perspectiva arquitetural da Helix não substitui estruturas formais de governança, políticas corporativas ou processos de gestão de risco. Seu papel é oferecer uma lente adicional que facilita a compreensão de como a maturidade decisória se desenvolve e como essa maturidade se articula às camadas operacional e formativa que compõem a arquitetura mais ampla da resiliência cibernética.

7.6 Integração entre os Domínios

Os domínios descritos nas subseções anteriores — ambientes educacionais, desenvolvimento profissional, infraestrutura crítica e governança corporativa — são frequentemente tratados como áreas distintas, abordadas por iniciativas independentes e sustentadas por frameworks específicos. Essa segmentação é, em muitos aspectos, apropriada: cada domínio apresenta características próprias que justificam abordagens especializadas.

Entretanto, a perspectiva arquitetural da Helix sugere que a resiliência cibernética, considerada ao longo do ciclo de vida, emerge também da integração entre esses domínios. Estudantes formados em ambientes educacionais eventualmente ingressam em ambientes profissionais; profissionais que atuam em setores críticos podem, ao longo de suas trajetórias, assumir responsabilidades de governança; decisões executivas em contextos corporativos, por sua vez, influenciam as condições sob as quais estudantes e profissionais desenvolvem sua maturidade cibernética. Essa interconexão entre domínios não é secundária; é constitutiva da continuidade estrutural da resiliência cibernética ao longo do tempo.

A aplicação da Helix como lente arquitetural pode contribuir para a compreensão dessa integração entre domínios. Ao oferecer um vocabulário comum — curvas de maturidade, cinco níveis, transições críticas, variável de risco —, a Helix permite que iniciativas desenvolvidas em domínios distintos sejam analisadas sob uma perspectiva compartilhada, favorecendo a articulação entre elas. Essa articulação é particularmente relevante em contextos nos quais a fragmentação entre domínios produz descontinuidades que comprometem a resiliência cibernética ao longo do ciclo de vida.

A integração entre domínios, na perspectiva da Helix, não implica homogeneização nem substituição de abordagens especializadas. Envolve o reconhecimento de que a resiliência cibernética é, em essência, capacidade que perpassa domínios específicos e se desenvolve por meio da continuidade estrutural entre eles. A arquitetura Helix oferece uma lente que facilita a observação e a articulação dessa continuidade, complementando — sem substituir — as abordagens específicas de cada domínio.

A próxima seção apresenta formas específicas de integração complementar entre a Arquitetura Helix e os frameworks consolidados descritos na Seção 2, desenvolvendo em maior detalhe a relação conceitual entre a Helix e o ecossistema de referências em cibersegurança.

8. Integração Complementar com Frameworks Estabelecidos

As seções anteriores estabeleceram a fundamentação conceitual da Arquitetura de Resiliência Cibernética Helix, as três curvas de maturidade, o modelo de maturidade em cinco níveis, as transições críticas ao longo do ciclo de vida e os domínios de aplicação em que a Helix pode ser utilizada de modo complementar. Esta seção desenvolve, em maior detalhe, as formas específicas de integração complementar entre a Helix e os frameworks consolidados descritos na Seção 2. Enquanto a Seção 2 apresentou cada framework de modo descritivo, e a Seção 3.5 estabeleceu a relação conceitual geral entre a Helix e o ecossistema de frameworks, esta seção articula como a integração opera, na prática, para cada framework individualmente, seguida de uma síntese sobre o uso integrado de múltiplos frameworks.

8.1 Fundamentos da Integração Complementar

A integração complementar entre a Helix e os frameworks consolidados se assenta sobre três premissas fundacionais que decorrem dos princípios arquiteturais apresentados na Seção 3.

A primeira premissa é que a Helix opera em uma camada conceitual distinta da camada dos frameworks consolidados. Os frameworks definem o que precisa ser endereçado em suas respectivas dimensões — funções, competências, controles, conteúdo educacional ou processos de governança. A Helix aborda como a maturidade para exercer esses elementos progride ao longo do ciclo de vida humano e institucional. Trata-se de questões distintas, mas relacionadas, e ambas são necessárias a uma compreensão completa da resiliência cibernética.

A segunda premissa é que a integração complementar não implica relação hierárquica. A Helix não se posiciona acima nem abaixo dos frameworks consolidados; ocupa uma camada arquitetural paralela que se intersecciona com cada framework em pontos específicos de conexão. Esse posicionamento paralelo assegura que a adoção da Helix não exige modificação no modo como os frameworks consolidados são aplicados em seus respectivos contextos.

A terceira premissa é que a integração com a Helix é aditiva, e não substitutiva. Organizações, instituições e ambientes educacionais que já aplicam um ou mais frameworks consolidados continuam a aplicá-los do modo habitual. A Helix contribui com uma lente adicional pela qual a maturidade necessária à sustentação desses frameworks ao longo do tempo se torna observável, mensurável e sistematicamente estruturada ao longo do ciclo de vida.

A tabela a seguir sintetiza as formas específicas de integração complementar entre a Helix e cada um dos frameworks consolidados descritos na Seção 2. Cada uma das subseções subsequentes (8.2 a 8.6) desenvolve uma linha dessa síntese em maior profundidade conceitual.

Tabela 1. Integração Complementar entre a Helix e os Frameworks Estabelecidos

Framework	Dimensão Primária Endereçada	Contribuição Complementar da Helix	Curva(s) Helix de Interseção Primária
NIST Cybersecurity Framework 2.0	Funções organizacionais de cibersegurança (Govern, Identify, Protect, Detect, Respond, Recover)	Perspectiva arquitetural sobre como a maturidade para executar essas funções progride ao longo do ciclo de vida das pessoas e instituições que as implementam	Operacional e de Governança
ISO/IEC 27001	Sistema de gestão da segurança da informação (SGSI) baseado em risco e melhoria contínua	Perspectiva arquitetural sobre como a maturidade humana e institucional necessária à sustentação do sistema de gestão evolui ao longo do tempo	Operacional e de Governança
NICE Workforce Framework	Competências profissionais, conhecimentos, habilidades e papéis de trabalho em cibersegurança	Perspectiva arquitetural sobre como a maturidade para exercer competências profissionais se desenvolve progressivamente, da exposição formativa à responsabilidade de governança	Formativa e Operacional
CSTA K-12 Computer Science Standards	Padrões educacionais de ciência da computação e cibersegurança para educação básica e média	Perspectiva arquitetural sobre como o comportamento digital desenvolvido em contextos formativos se conecta progressivamente aos estágios subsequentes do ciclo de vida	Formativa
ISACA COBIT	Governança e gestão de TI corporativa, incluindo dimensões de cibersegurança	Perspectiva arquitetural sobre como a maturidade decisória para exercer responsabilidade de governança em cibersegurança evolui ao longo da trajetória do tomador de decisão	Governança

Esta tabela não substitui a articulação detalhada apresentada em cada subseção. Serve como referência visual do posicionamento complementar da Helix dentro do ecossistema mais amplo de frameworks, possibilitando ao leitor situar as discussões subsequentes em uma visão estrutural compartilhada.

8.2 Helix e o NIST Cybersecurity Framework

O NIST Cybersecurity Framework 2.0 estrutura a cibersegurança organizacional em torno de seis funções centrais — Govern, Identify, Protect, Detect, Respond e Recover —, que descrevem atividades essenciais ao longo do ciclo de gestão da cibersegurança. Essas funções são organizadas em categorias, subcategorias e referências informativas que possibilitam aplicação em organizações de diferentes portes, setores e níveis de maturidade.

A integração complementar entre a Helix e o NIST CSF opera na interseção entre a descrição funcional oferecida pelo framework e a progressão da maturidade humana e institucional necessária à execução efetiva dessas funções. O NIST CSF especifica o que as organizações fazem para gerir a cibersegurança; a Helix oferece uma lente para compreender como a maturidade para executar essas atividades se desenvolve ao longo do ciclo de vida das pessoas que as operam.

Essa relação complementar é particularmente evidente na função Govern, introduzida no NIST CSF 2.0. A função Govern aborda o estabelecimento, a comunicação e o monitoramento de estratégias, expectativas e políticas de gestão de risco cibernético. A maturidade decisória requerida ao exercício efetivo da função Govern — descrita pela curva de governança da Helix — evolui ao longo da trajetória do tomador de decisão, apoiando-se em experiência operacional anterior e em consolidação formativa precedente. Um tomador de decisão no Nível 5 da Helix (Liderança Arquitetural) exerce a função Govern com perspectiva sistêmica e impacto estruturado sobre estágios anteriores do ciclo de vida, enquanto um tomador de decisão no Nível 3 da Helix dentro da curva de governança exerce a mesma função com capacidade estratégica emergente, mas ainda não plenamente consolidada.

De modo análogo, as funções Protect, Detect e Respond são executadas predominantemente por profissionais que atuam na curva operacional da Helix. A qualidade com que essas funções são desempenhadas depende não apenas dos controles e procedimentos definidos pelo NIST CSF, mas também da maturidade operacional dos profissionais que os aplicam — dimensão arquitetural que a Helix torna explícita. Organizações que aplicam o NIST CSF podem utilizar a perspectiva da Helix para observar como a progressão da maturidade operacional influencia a execução efetiva das funções do framework ao longo do tempo.

8.3 Helix e a ISO/IEC 27001

A ISO/IEC 27001 estabelece os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI), oferecendo estrutura de gestão baseada em abordagem orientada a risco com ciclo de melhoria contínua. A norma é amplamente adotada como referência para certificação formal, conformidade regulatória e alinhamento contratual em ambientes corporativos e governamentais.

A integração complementar entre a Helix e a ISO/IEC 27001 opera na interseção entre a formalização sistêmica oferecida pela norma e a maturidade humana e institucional necessária à sustentação desse sistema ao longo do tempo. A ISO/IEC 27001 especifica os requisitos estruturais de um SGSI; a Helix oferece uma lente para compreender como a maturidade das pessoas e instituições que operam e governam o SGSI evolui progressivamente.

Essa relação complementar é particularmente evidente no ciclo de melhoria contínua central à ISO/IEC 27001. A melhoria contínua não é apenas requisito procedimental; depende da maturidade progressiva dos profissionais que executam o SGSI (curva operacional da Helix) e da maturidade decisória dos líderes que sustentam o sistema estrategicamente (curva de governança da Helix). Um SGSI implementado por profissionais no Nível 4 da Helix dentro da curva operacional tende a produzir resultados — ao longo do tempo — distintos dos produzidos por um SGSI implementado por profissionais no Nível 2, ainda que os requisitos técnicos da norma sejam formalmente atendidos em ambos os casos.

Adicionalmente, a abordagem orientada a risco da ISO/IEC 27001 alinha-se diretamente à lógica de mensuração baseada em risco da Helix apresentada na Seção 5.3. Ambas reconhecem que a cibersegurança trata, fundamentalmente, da redução da probabilidade e do impacto de eventos adversos. A lente Helix amplia esse reconhecimento ao tornar explícito que a redução do risco no contexto de um SGSI depende da progressão da maturidade humana e institucional — e não apenas da aplicação formal dos controles especificados pela norma.

8.4 Helix e o NICE Workforce Framework

O NICE Workforce Framework for Cybersecurity estabelece taxonomia abrangente de competências, conhecimentos, habilidades e papéis de trabalho em cibersegurança. Oferece linguagem comum para que empregadores, educadores e profissionais descrevam, desenvolvam e avaliem capacidades em cibersegurança, ao longo de programas educacionais, trilhas de carreira e iniciativas de desenvolvimento de força de trabalho.

A integração complementar entre a Helix e o NICE opera na interseção entre a estrutura de competências definida pelo framework e a progressão da maturidade requerida ao exercício consistente dessas competências ao longo do tempo. O NICE especifica quais competências são requeridas para cada papel de trabalho em cibersegurança; a Helix oferece uma lente para compreender como a maturidade para exercer essas competências se desenvolve progressivamente ao longo do ciclo de vida humano.

Essa relação complementar é particularmente evidente na transição entre formação e prática operacional. Profissionais que desenvolvem as competências descritas pelo NICE frequentemente transitam de contextos educacionais ou de início de carreira para ambientes operacionais nos quais essas competências precisam ser sustentadas sob pressão operacional. A perspectiva da Helix sobre as transições críticas (Seção 6) torna esse momento arquitetural explícito, oferecendo modo estruturado de observar se as competências formalmente adquiridas se traduzem em prática profissional consistente.

Adicionalmente, a organização dos papéis de trabalho do NICE Framework mapeia naturalmente sobre os níveis de maturidade da Helix dentro da curva operacional. Papéis de nível inicial podem com frequência se intersectar com os Níveis 1–2 da Helix na curva operacional, papéis de nível intermediário com os Níveis 3–4, e papéis de nível sênior com os Níveis 4–5, com possível interseção na curva de governança. Esse mapeamento não implica que a Helix substitua a taxonomia do NICE; indica que os dois frameworks podem ser utilizados em conjunto para observar tanto a aquisição de competências (NICE) quanto a progressão da maturidade (Helix) ao longo da trajetória profissional.

8.5 Helix e os CSTA K-12 Computer Science Standards

Os CSTA K-12 Computer Science Standards estabelecem diretrizes para o ensino de ciência da computação desde a primeira infância até o ensino médio, organizando conceitos fundamentais em áreas como Sistemas Computacionais, Redes e Internet, Dados e Análise, Algoritmos e Programação, e Impactos da Computação. Entre as dimensões abordadas, os padrões cobrem explicitamente a cibersegurança, a privacidade digital, a ética computacional e a cidadania digital.

A integração complementar entre a Helix e os CSTA Standards opera na interseção entre o conteúdo educacional definido pelos padrões e a perspectiva arquitetural sobre como as fundações comportamentais desenvolvidas por meio desse conteúdo se conectam aos estágios subsequentes do ciclo de vida. O CSTA especifica o que os estudantes aprendem sobre

computação e cibersegurança na educação básica; a Helix oferece uma lente para compreender como esse aprendizado inicial se traduz em padrões comportamentais sustentados que influenciam estágios operacionais e de governança posteriores.

Essa relação complementar é particularmente evidente na curva formativa da Helix. Estudantes que avançam pelos CSTA Standards desenvolvem competências digitais e comportamentos seguros que podem ser observados, pela lente Helix, como progressão ao longo dos Níveis 1 a 3 dentro da curva formativa. A perspectiva da Helix acrescenta ao framework educacional dos CSTA o reconhecimento explícito de que essas fundações comportamentais têm valor arquitetural que vai além do contexto educacional — constituem a base sobre a qual a maturidade operacional e de governança são posteriormente edificadas.

Adicionalmente, a perspectiva da Helix sobre a transição da curva formativa para a operacional (Seção 6.2) é particularmente relevante para iniciativas educacionais alinhadas aos CSTA que visam preparar estudantes para trajetórias profissionais em cibersegurança e tecnologia. Programas educacionais que aplicam os CSTA podem utilizar a lente Helix para observar se os padrões comportamentais desenvolvidos durante a formação possuem consistência suficiente (Nível 3 da Helix) para sustentar transição efetiva aos ambientes operacionais subsequentes.

8.6 Helix e o ISACA COBIT

O ISACA COBIT oferece um framework para a governança e a gestão de TI corporativa, articulando princípios de governança, objetivos de gestão, práticas e processos que sustentam o alinhamento entre tecnologia da informação e objetivos de negócio. O COBIT inclui dimensões específicas relacionadas à cibersegurança e à gestão de risco, o que o torna particularmente relevante para organizações que integram a cibersegurança a estruturas mais amplas de governança corporativa.

A integração complementar entre a Helix e o COBIT opera na interseção entre a estrutura de governança definida pelo framework e a maturidade decisória requerida ao exercício efetivo da responsabilidade de governança. O COBIT especifica os princípios, objetivos e processos para a governança de TI; a Helix oferece uma lente para compreender como a maturidade dos tomadores de decisão para exercer responsabilidade de governança em cibersegurança evolui progressivamente ao longo de sua trajetória.

Essa relação complementar é particularmente evidente na curva de governança da Helix, que aborda diretamente a dimensão decisória estruturada pelo COBIT. Tomadores de decisão que exercem os princípios de governança do COBIT operam em diferentes níveis da Helix dentro da curva de governança — desde o engajamento inicial em decisões estratégicas (Nível 1 da Helix dentro da curva de governança) até a liderança arquitetural plena (Nível 5). Organizações que aplicam o COBIT podem utilizar a perspectiva da Helix para observar como a maturidade decisória progride ao longo do tempo, para além da aplicação formal dos processos do COBIT.

Adicionalmente, a perspectiva da Helix sobre a transição da curva operacional para a curva de governança (Seção 6.3) é particularmente relevante para organizações que desenvolvem futuros líderes de cibersegurança. O COBIT estrutura o que a governança requer; a Helix oferece um modo estruturado de observar se a transição da experiência operacional à tomada de decisão estratégica é adequadamente apoiada — preocupação arquitetural que o próprio COBIT não aborda explicitamente.

8.7 Uso Integrado de Múltiplos Frameworks

Na prática, organizações, instituições e ambientes educacionais raramente aplicam um único framework consolidado de modo isolado. Instituições educacionais podem alinhar currículos aos CSTA Standards enquanto preparam estudantes para trajetórias profissionais descritas pelo NICE; organizações podem implementar a ISO/IEC 27001 para certificação formal ao mesmo tempo em que utilizam o NIST CSF como referência operacional e integram a governança por meio do COBIT. A Arquitetura de Resiliência Cibernética Helix, como perspectiva arquitetural, sustenta o uso integrado de múltiplos frameworks ao oferecer uma lente comum que observa a progressão da maturidade ao longo do ciclo de vida, independentemente de quais frameworks específicos sejam aplicados.

Essa capacidade integradora decorre do posicionamento arquitetural da Helix estabelecido na Seção 3. Como a Helix não prescreve controles, competências ou processos de governança específicos a um framework em particular, ela pode ser aplicada em conjunto com qualquer combinação de frameworks consolidados sem produzir conflitos ou redundâncias. Uma organização que aplica simultaneamente NIST CSF, ISO/IEC 27001 e COBIT — configuração comum em setores regulados — pode utilizar a perspectiva da Helix para observar como a maturidade progride ao longo dos três frameworks como camadas integradas, em vez de domínios separados de conformidade.

O vocabulário comum oferecido pela Helix — curvas de maturidade, cinco níveis, transições críticas, mensuração baseada em risco — possibilita comparação e articulação entre frameworks de modos que esses frameworks, aplicados isoladamente, não oferecem naturalmente. Isso é particularmente relevante em contextos nos quais as transições entre formação educacional (CSTA), prática profissional (NICE, NIST CSF) e governança executiva (COBIT) requerem atenção estruturada. A lente Helix não reduz a especificidade de cada framework; contribui com uma camada de coerência arquitetural que os conecta ao longo do ciclo de vida das pessoas e instituições que os aplicam.

O uso integrado da Helix com frameworks consolidados reflete sua natureza complementar. Em vez de competir com referências existentes, a Helix contribui com uma camada arquitetural à sua aplicação combinada, ao tornar explícita a dimensão arquitetural da progressão da maturidade — dimensão que, sem uma lente arquitetural, tende a permanecer implícita e dispersa entre os domínios separados de cada framework. A próxima seção apresenta o ecossistema de implementação atualmente em desenvolvimento, que operacionaliza a aplicação da Helix em contextos educacionais, profissionais e de governança.

9. Ecossistema de Implementação em Desenvolvimento

As seções anteriores apresentaram a fundamentação conceitual da Arquitetura de Resiliência Cibernética Helix, suas três curvas de maturidade, o modelo de maturidade em cinco níveis, as transições críticas ao longo do ciclo de vida, os domínios de aplicação e as formas de integração complementar com frameworks consolidados. Esta seção apresenta o ecossistema de implementação atualmente em desenvolvimento, constituído por iniciativas estruturadas que operacionalizam a aplicação da Helix em diferentes camadas do ciclo de vida. O ecossistema não é apresentado como conjunto fechado de produtos ou serviços; é apresentado como contexto de pesquisa-ação, no qual os princípios arquiteturais do modelo são continuamente aplicados, observados e refinados.

9.1 Visão Geral do Ecossistema

O ecossistema de implementação da Helix é constituído por iniciativas desenvolvidas com o propósito de operacionalizar, em contextos reais, os princípios arquiteturais do modelo. Cada iniciativa atua predominantemente em uma das três camadas do ciclo de vida representadas pelas curvas de maturidade descritas na Seção 4. Em conjunto, as iniciativas compõem um arranjo estruturado que busca sustentar a continuidade da resiliência cibernética desde a formação inicial até a responsabilidade de governança.

A organização do ecossistema segue a lógica arquitetural da Helix. Iniciativas voltadas à curva formativa oferecem contextos estruturados para o desenvolvimento comportamental pré-operacional. Iniciativas voltadas à curva operacional oferecem conteúdo e estruturas que apoiam a integração profissional em ambientes técnicos. Iniciativas voltadas à curva de governança oferecem recursos alinhados à maturidade decisória em cibersegurança. Essa organização reflete a premissa arquitetural de que a resiliência cibernética se desenvolve por meio da continuidade estrutural entre essas três camadas, e não por meio de iniciativas isoladas em cada uma delas.

Quatro iniciativas compõem o ecossistema atualmente em desenvolvimento: a Cyber Heroes League, voltada à curva formativa por meio de narrativa educativa; a plataforma Be a Cyber Hero, voltada à curva formativa por meio de conteúdo estruturado; a plataforma Stay Cyber Aware, voltada à curva operacional por meio de conteúdo orientado ao ambiente de trabalho para profissionais de cibersegurança; e a plataforma Be a Cyber Leader, voltada à curva de governança por meio de conteúdo direcionado a tomadores de decisão e líderes de

cibersegurança. As subseções seguintes descrevem cada uma dessas iniciativas em sua dimensão arquitetural, evidenciando como operacionalizam os elementos da Helix.

A apresentação do ecossistema nesta seção não pretende ser exaustiva, nem busca descrever todas as dimensões operacionais de cada iniciativa. O propósito é ilustrar, em termos arquiteturais, como os princípios da Helix se manifestam em contextos concretos de desenvolvimento e aplicação. O ecossistema está em processo contínuo de desenvolvimento, e as iniciativas aqui descritas refletem seu estado atual, sem prejuízo de evoluções subsequentes.

9.2 Iniciativas da Curva Formativa

A curva formativa, conforme descrita na Seção 4.2, corresponde ao desenvolvimento pré-operacional do comportamento e da consciência digital. Duas iniciativas do ecossistema atuam predominantemente nessa curva, com propósitos arquiteturais distintos e complementares: a Cyber Heroes League, voltada à introdução narrativa de conceitos de cibersegurança; e a plataforma Be a Cyber Hero, voltada ao desenvolvimento estruturado da consciência digital.

9.2.1 Cyber Heroes League: Introdução Formativa Baseada em Narrativa

A Cyber Heroes League é uma iniciativa formativa constituída por uma trilogia de livros que apresenta conceitos de cibersegurança por meio de estruturas narrativas ficcionais. A proposta arquitetural dessa iniciativa é atuar no estágio inicial da curva formativa, correspondente aos Níveis 1 e 2 do modelo Helix, em que o indivíduo estabelece seu primeiro contato estruturado com temas de cibersegurança e inicia o desenvolvimento de padrões comportamentais iniciais de consciência digital.

A escolha do formato narrativo reflete uma premissa pedagógica específica: o engajamento inicial com a cibersegurança é facilitado quando os conceitos são apresentados por meio de personagens, enredos e cenários que permitem ao leitor construir uma compreensão progressiva sem exposição direta a vocabulário técnico especializado. Essa abordagem é particularmente adequada a públicos em fases iniciais de exposição digital, incluindo crianças, adolescentes e jovens que se aproximam do domínio da cibersegurança pela primeira vez.

Do ponto de vista arquitetural, a Cyber Heroes League contribui para a operacionalização da curva formativa da Helix em dois aspectos principais. Primeiro, oferece um vetor de exposição estruturada a conceitos fundamentais de cibersegurança em formato

acessível, favorecendo a transição do Nível 1 (Exposição Fundacional) para o Nível 2 (Formação Comportamental). Segundo, estabelece uma referência narrativa que pode ser revisitada em contextos posteriores de desenvolvimento, favorecendo a continuidade entre o engajamento inicial e os estágios subsequentes da formação.

9.2.2 Be a Cyber Hero: Desenvolvimento Formativo Estruturado

A plataforma Be a Cyber Hero é uma iniciativa formativa constituída por conteúdo estruturado voltado ao desenvolvimento progressivo da consciência digital e dos padrões comportamentais de cibersegurança. A proposta arquitetural dessa iniciativa é atuar em um estágio ligeiramente mais avançado da curva formativa em relação à Cyber Heroes League, correspondente principalmente aos Níveis 2 e 3 do modelo Helix, em que o indivíduo consolida padrões comportamentais iniciais e avança em direção à consistência comportamental estável.

Enquanto a Cyber Heroes League opera primariamente pelo engajamento narrativo, a Be a Cyber Hero opera pelo desenvolvimento estruturado por meio de conteúdo explícito — ensaios, artigos, recursos educativos e reflexões orientados à internalização da responsabilidade digital. Essa diferença de formato reflete uma diferença arquitetural: a Cyber Heroes League favorece a exposição inicial e a formação do interesse, enquanto a Be a Cyber Hero favorece a consolidação comportamental por meio do contato sustentado com conteúdo estruturado sobre cibersegurança.

Do ponto de vista arquitetural, a plataforma Be a Cyber Hero contribui para a operacionalização da curva formativa da Helix em três aspectos principais. Primeiro, oferece estrutura de conteúdo que favorece o avanço do Nível 2 (Formação Comportamental) ao Nível 3 (Consistência Comportamental), por meio da exposição continuada a reflexões sobre comportamento digital responsável. Segundo, estabelece referências conceituais que podem apoiar a eventual transição da curva formativa para a operacional, abordada na Seção 6.2. Terceiro, oferece um vetor de continuidade em relação à exposição inicial proporcionada pela Cyber Heroes League, possibilitando progressão coerente dentro da curva formativa.

A complementaridade entre as duas iniciativas formativas reflete uma premissa arquitetural da Helix: o desenvolvimento formativo não ocorre por meio de exposição discreta, mas pela sustentação estruturada ao longo do tempo, articulando formatos e abordagens apropriados a cada estágio da maturidade inicial.

9.3 Iniciativa da Curva Operacional: Stay Cyber Aware

A curva operacional, conforme descrita na Seção 4.3, corresponde à integração do comportamento digital em ambientes profissionais reais. A plataforma Stay Cyber Aware é a iniciativa do ecossistema voltada a essa camada do ciclo de vida, atuando primariamente nos Níveis 3 e 4 do modelo Helix — estágios em que profissionais consolidam consistência comportamental em ambientes de trabalho e avançam em direção à integração operacional plena.

A Stay Cyber Aware é constituída por conteúdo estruturado e orientado ao ambiente de trabalho, voltado a profissionais que atuam em ambientes organizacionais nos quais a cibersegurança constitui responsabilidade compartilhada. A plataforma aborda temas relacionados à consciência operacional em contextos corporativos, à aplicação prática de princípios de cibersegurança em contextos corporativos e à manutenção de comportamentos seguros em cenários de pressão operacional. Sua proposta é apoiar a transição entre formação inicial e prática profissional consistente, bem como sustentar a continuidade comportamental ao longo da trajetória do profissional em ambientes operacionais.

Do ponto de vista arquitetural, a Stay Cyber Aware contribui para a operacionalização da curva operacional da Helix em três aspectos principais. Primeiro, oferece um vetor de sustentação comportamental em contextos profissionais, reforçando a manutenção de padrões desenvolvidos nas fases anteriores do ciclo de vida. Segundo, estabelece um espaço estruturado de reflexão sobre situações operacionais concretas, favorecendo a consolidação da consistência comportamental (Nível 3) e o avanço à integração operacional (Nível 4). Terceiro, opera como ponte conceitual entre formação e prática, conectando conceitos introduzidos em contextos formativos a sua aplicação em ambientes de responsabilidade profissional.

A iniciativa Stay Cyber Aware se relaciona diretamente à transição da curva formativa para a operacional, descrita na Seção 6.2. Ao oferecer conteúdo específico para profissionais que atuam em ambientes corporativos, a plataforma aborda o momento arquitetural em que a maturidade desenvolvida em contextos formativos precisa ser sustentada sob as condições reais da prática profissional.

9.4 Iniciativa da Curva de Governança: Be a Cyber Leader

A curva de governança, conforme descrita na Seção 4.4, corresponde ao alinhamento da resiliência cibernética com a liderança, a responsabilidade executiva e a tomada de decisão estratégica. A plataforma Be a Cyber Leader é a iniciativa do ecossistema voltada a essa camada do ciclo de vida, atuando primariamente nos Níveis 4 e 5 do modelo Helix — estágios

em que tomadores de decisão consolidam capacidade decisória em cibersegurança e avançam em direção à liderança arquitetural sistêmica.

A Be a Cyber Leader é constituída por conteúdo estruturado voltado a tomadores de decisão, líderes executivos e profissionais em posições de responsabilidade estratégica em cibersegurança. A plataforma aborda temas relacionados à inserção do risco cibernético no centro da tomada de decisão estratégica, à articulação entre cibersegurança e objetivos institucionais amplos, e à estruturação de mecanismos de prestação de contas que sustentem a resiliência ao longo do tempo. Sua proposta é apoiar o desenvolvimento da maturidade decisória em cibersegurança e a consolidação da visão sistêmica requerida em contextos de governança.

Do ponto de vista arquitetural, a Be a Cyber Leader contribui para a operacionalização da curva de governança da Helix em três aspectos principais. Primeiro, oferece um espaço estruturado para o desenvolvimento da maturidade decisória, apoiando a transição da curva operacional para a de governança descrita na Seção 6.3. Segundo, estabelece referências conceituais para a articulação entre decisões estratégicas de cibersegurança e as realidades operacionais que essas decisões influenciam. Terceiro, opera como vetor de consolidação da liderança arquitetural (Nível 5), em que a maturidade individual se converte em capacidade de estruturar sistemicamente as condições de resiliência em organizações e ecossistemas.

A iniciativa Be a Cyber Leader se relaciona diretamente à implicação arquitetural apresentada na Seção 6.4, segundo a qual decisões de governança estruturam as condições sob as quais profissionais operam e indivíduos são formados. Ao oferecer conteúdo específico para líderes e tomadores de decisão, a plataforma aborda a camada do ciclo de vida cuja influência recíproca se estende às curvas anteriores, reforçando a continuidade estrutural da arquitetura.

9.5 O Ecossistema como Contexto de Pesquisa-Ação

O ecossistema de implementação descrito nesta seção não constitui conjunto fechado de soluções, nem busca, neste estágio, validar empiricamente a Arquitetura de Resiliência Cibernética Helix em sua totalidade. Constitui, antes, contexto de pesquisa-ação no qual os princípios arquiteturais do modelo são continuamente aplicados, observados e refinados. Essa orientação reflete o caráter desenvolvimental da arquitetura, estabelecido na Seção 3, segundo o qual a resiliência cibernética é capacidade em evolução, e não condição estática que possa ser garantida por arranjos definitivos.

Três características do ecossistema merecem ênfase nesse contexto. A primeira é seu caráter progressivo: as iniciativas que o compõem encontram-se em diferentes estágios de desenvolvimento, e sua articulação reflete um processo contínuo de construção, ajuste e aprofundamento. A segunda é sua orientação arquitetural: cada iniciativa é concebida não como produto isolado, mas como camada específica de um arranjo mais amplo, voltado à continuidade estrutural da resiliência cibernética ao longo do ciclo de vida. A terceira é sua abertura conceitual: o ecossistema é intencionalmente mantido em desenvolvimento contínuo, possibilitando a incorporação de novas iniciativas, ajustes às existentes e refinamentos resultantes da observação prática de sua aplicação.

A existência do ecossistema também oferece oportunidades de pesquisa futura relacionadas à própria Helix. A observação continuada da aplicação das iniciativas em contextos reais pode gerar informações relevantes sobre a progressão dos cinco níveis de maturidade ao longo das três curvas, sobre as condições que favorecem ou restringem as transições críticas entre as curvas e sobre o impacto sistêmico da articulação entre as camadas formativa, operacional e de governança. Essas oportunidades de pesquisa são discutidas em maior detalhe na Seção 10.

Em essência, o ecossistema descrito nesta seção ilustra a aplicação concreta dos princípios da Helix em contextos reais, sem buscar esgotar as formas possíveis de operacionalização do modelo. Representa um estado atual de desenvolvimento, a partir do qual refinamentos contínuos — tanto nas iniciativas quanto na própria arquitetura conceitual — permanecem em curso. A próxima seção apresenta as considerações finais do artigo, incluindo síntese das contribuições, reconhecimento das limitações e direções para trabalhos futuros.

10. Considerações Finais e Trabalhos Futuros

Esta seção oferece as considerações finais do artigo, incluindo a síntese das principais contribuições, o reconhecimento explícito das limitações do trabalho, as direções para pesquisas futuras e reflexões finais que situam a Arquitetura de Resiliência Cibernética Helix no contexto mais amplo de sua trajetória de desenvolvimento e da contribuição que se propõe a oferecer ao campo da resiliência cibernética.

10.1 Síntese das Contribuições

Este artigo apresentou a Arquitetura de Resiliência Cibernética Helix como uma arquitetura conceitual baseada em ciclo de vida, estruturada em torno de três curvas de maturidade interdependentes — formativa, operacional e de governança — e de um modelo de progressão em cinco níveis, fundamentado na lógica da redução observável do risco. Ao longo das seções anteriores, a arquitetura foi desenvolvida em sua fundamentação conceitual, em seus princípios, em sua lógica de mensuração, em suas transições críticas e em seus domínios de aplicação, bem como em sua relação complementar com os frameworks consolidados em cibersegurança.

A contribuição central deste trabalho é de natureza arquitetural. A Helix não propõe novos controles técnicos, não redefine competências profissionais já estabelecidas e não prescreve processos específicos de governança. Sua contribuição reside em oferecer uma lente estruturada para compreender como os elementos já definidos pelos frameworks consolidados — NIST CSF, ISO/IEC 27001, NICE Framework, CSTA K-12 Standards, ISACA COBIT, entre outros — se conectam progressivamente ao longo do ciclo de vida humano e institucional. Essa perspectiva complementar busca contribuir para a compreensão da resiliência cibernética não apenas como um conjunto de capacidades estáticas a serem implementadas, mas como capacidade em evolução que emerge da continuidade estrutural entre formação humana, integração operacional e responsabilidade de governança.

Seis contribuições específicas decorrem dessa proposta arquitetural. A primeira é a fundamentação conceitual da Helix como arquitetura, ancorada em quatro princípios — centrada no humano, progressiva, arquiteturalmente integrada e mensurável. A segunda é a descrição das três curvas de maturidade como dimensões interdependentes da resiliência cibernética, unificadas pela variável comum da maturidade do indivíduo em relação à exposição ao risco cibernético. A terceira é a proposição de um modelo de maturidade em cinco

níveis, transversal às três curvas e fundamentado na redução observável do risco em cenários reais. A quarta é a identificação das transições críticas entre as curvas como elementos arquiteturais específicos, cuja qualidade influencia significativamente a continuidade da resiliência cibernética ao longo do ciclo de vida. A quinta é a apresentação de domínios de aplicação em que a arquitetura pode ser utilizada de modo complementar a iniciativas existentes. A sexta é a descrição de um ecossistema de implementação atualmente em desenvolvimento, que operacionaliza os princípios da arquitetura em contextos formativos, operacionais e de governança.

Em conjunto, essas contribuições buscam oferecer uma perspectiva arquitetural coerente e defensável, articulada ao ecossistema de frameworks consolidados e orientada à continuidade estrutural da resiliência cibernética ao longo do tempo.

10.2 Limitações Reconhecidas

O presente trabalho apresenta limitações que são explicitamente reconhecidas e que constituem, em conjunto, agenda natural para o desenvolvimento contínuo da Arquitetura de Resiliência Cibernética Helix.

A primeira limitação diz respeito à natureza do trabalho apresentado. Este artigo apresenta a Helix como arquitetura conceitual fundamentada na observação continuada da prática profissional em cibersegurança e em sua articulação com frameworks consolidados. Essa fundamentação, embora consistente, não substitui validação empírica em larga escala, que ainda não foi conduzida de modo sistemático. As observações apresentadas refletem o estado atual do desenvolvimento conceitual da arquitetura e devem ser entendidas como ponto de partida para investigações subsequentes, e não como afirmações conclusivas sobre o comportamento do modelo em todos os contextos possíveis de aplicação.

A segunda limitação refere-se à necessidade de estudos longitudinais para observar a progressão entre as curvas de maturidade. A lógica arquitetural da Helix pressupõe que a continuidade estrutural entre formação, operação e governança se manifesta ao longo de trajetórias humanas e institucionais que se estendem por períodos prolongados. A observação sistemática dessa continuidade requer estudos conduzidos ao longo do tempo, capazes de acompanhar indivíduos e instituições em múltiplos estágios do ciclo de vida. Tais estudos, embora metodologicamente desafiadores, são essenciais para o refinamento do modelo e para a validação empírica da lógica de progressão proposta.

A terceira limitação refere-se à necessidade de adaptação contextual entre setores e ambientes regulatórios distintos. Embora a Helix seja proposta como arquitetura de aplicação ampla, sua operacionalização em setores específicos — como infraestrutura crítica, serviços financeiros, saúde ou educação — pode requerer ajustes contextuais que respeitem as particularidades regulatórias, culturais e operacionais de cada ambiente. A arquitetura, em sua formulação atual, oferece estrutura geral; sua aplicação efetiva em contextos específicos depende de refinamentos que preservem a coerência arquitetural ao mesmo tempo em que adaptem sua manifestação observável às condições particulares de cada setor.

A quarta limitação refere-se à necessidade de aprofundamento metodológico adicional para a padronização da avaliação entre domínios distintos. A metodologia tríplice de avaliação proposta na Seção 5.4 — avaliação da compreensão conceitual, avaliação baseada em cenários e observação longitudinal — oferece base defensável para a classificação da maturidade, mas requer instrumentos específicos, protocolos estruturados e critérios de padronização que possibilitem aplicação consistente em diferentes contextos. O desenvolvimento desses instrumentos constitui campo aberto de pesquisa metodológica, complementar ao refinamento conceitual da arquitetura.

Essas quatro limitações, consideradas em conjunto, não invalidam a contribuição arquitetural da Helix. Indicam, antes, que a arquitetura é estruturada, aplicável e conceitualmente consistente, mas permanece aberta a validação ampliada, refinamento metodológico e observação em contextos diversos. A apresentação deste artigo reflete um estágio específico dessa trajetória de desenvolvimento, e não seu encerramento.

10.3 Direções para Pesquisas Futuras

As limitações reconhecidas na subseção anterior sugerem naturalmente direções para pesquisas futuras relacionadas ao desenvolvimento contínuo da Arquitetura de Resiliência Cibernética Helix. Essas direções não são apresentadas como agenda fechada, mas como campo aberto de investigação, que pode ser explorado por pesquisadores, educadores e profissionais interessados na aplicação, na crítica e no refinamento do modelo.

Uma primeira direção consiste na validação empírica das três curvas de maturidade em diversos contextos de aplicação. Estudos específicos focados na observação da manifestação das curvas formativa, operacional e de governança em diferentes setores e ambientes podem contribuir para o refinamento da arquitetura e para a identificação de padrões que reforcem ou revisem suas premissas atuais. Tais estudos podem adotar abordagens qualitativas,

quantitativas ou de métodos mistos, dependendo do contexto específico de aplicação e das questões de pesquisa formuladas.

Uma segunda direção consiste em estudos longitudinais voltados à observação da progressão entre os níveis de maturidade e das transições críticas entre as curvas. A lógica arquitetural da Helix pressupõe continuidade estrutural ao longo do ciclo de vida; essa continuidade pode ser observada com maior precisão por estudos que acompanhem indivíduos, profissionais ou tomadores de decisão em múltiplos estágios de sua trajetória em cibersegurança. Tais estudos podem também contribuir para uma compreensão mais detalhada das condições que favorecem ou restringem as transições críticas identificadas na Seção 6.

Uma terceira direção consiste no desenvolvimento de instrumentos metodológicos específicos para a aplicação da metodologia de avaliação proposta na Seção 5.4. Esses instrumentos podem incluir protocolos para avaliação da compreensão conceitual, cenários estruturados para avaliação prática, indicadores comportamentais longitudinais e critérios de padronização que possibilitem comparação consistente entre contextos distintos. O desenvolvimento desses instrumentos pode ser conduzido de modo colaborativo, incorporando contribuições de pesquisadores, educadores, profissionais e instituições interessadas.

Uma quarta direção consiste na integração da Helix com frameworks não abordados explicitamente neste artigo, como CIS Controls, MITRE ATT&CK, outros padrões setoriais ou iniciativas regionais de cibersegurança. A arquitetura é, por sua natureza, compatível com múltiplos frameworks; sua articulação específica com referências não cobertas neste trabalho pode ampliar seu alcance e contribuir para sua consolidação como perspectiva arquitetural de aplicação ampla.

Uma quinta direção consiste na observação continuada do ecossistema de implementação descrito na Seção 9, como contexto adicional de pesquisa-ação que pode gerar informações relevantes sobre a aplicação dos princípios da arquitetura sob condições reais. Essa observação pode contribuir, ao longo do tempo, tanto para o refinamento das iniciativas quanto para o desenvolvimento da própria arquitetura conceitual, em processo bidirecional de evolução.

Essas cinco direções, entre outras possíveis, constituem campo aberto de investigação. Cada uma pode ser explorada de modo autônomo ou em articulação, conforme os interesses, recursos e contextos dos pesquisadores envolvidos. A Arquitetura de Resiliência Cibernética Helix, em sua formulação atual, é compatível com múltiplas abordagens metodológicas e

permanece aberta a contribuições que possam enriquecer seu desenvolvimento conceitual e prático.

10.4 Reflexões Finais

A Arquitetura de Resiliência Cibernética Helix foi originalmente desenvolvida em contexto de prática profissional e de propósito educativo, como resultado da observação continuada da cibersegurança ao longo de mais de duas décadas. Sua apresentação neste artigo reflete o esforço de refinar, estruturar e compartilhar essa arquitetura com as comunidades acadêmicas e profissionais interessadas em sua aplicação, crítica, validação e refinamento. Esse processo permanece conectado a um ecossistema de implementação em desenvolvimento, no qual os princípios da arquitetura continuam a ser observados e refinados.

Mais do que se propor como formulação definitiva, este trabalho constitui um convite à reflexão sobre como a resiliência cibernética se desenvolve progressivamente ao longo do ciclo de vida humano e institucional, e sobre como arquiteturas conceituais podem contribuir, de modo complementar aos frameworks consolidados, para essa compreensão. A resiliência cibernética, considerada em sua dimensão arquitetural, não é uma condição que possa ser simplesmente estabelecida; é uma capacidade que emerge e se sustenta por meio da continuidade estrutural entre comportamento humano, prática profissional e tomada de decisão estratégica, ao longo do tempo e em contextos diversos.

O campo da cibersegurança dispõe hoje de frameworks robustos que estruturam controles, competências, práticas educacionais e processos de governança em suas dimensões específicas. A Arquitetura de Resiliência Cibernética Helix é oferecida como perspectiva complementar a esse ecossistema de referências, com o propósito de ampliar a compreensão arquitetural da resiliência cibernética ao longo do tempo. Seu valor final dependerá do modo como ela for aplicada, discutida, criticada e refinada pelas comunidades acadêmicas e profissionais interessadas em suas premissas e em sua capacidade de contribuir para a continuidade estrutural da resiliência cibernética em contextos reais.

Este artigo, portanto, não encerra o desenvolvimento da Arquitetura de Resiliência Cibernética Helix. Apresenta um estágio de seu desenvolvimento, aberto a aprofundamentos, validações empíricas, adaptações contextuais e refinamentos metodológicos que possam, ao longo do tempo, enriquecer sua contribuição ao campo.

Referências

- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.
<https://doi.org/10.1016/j.ejor.2015.12.023>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. <https://arxiv.org/abs/1901.02672>
- Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management — A procedure model and its application. *Business & Information Systems Engineering*, 1(3), 213–222. <https://doi.org/10.1007/s12599-009-0044-5>
- Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience — Fundamentals for a definition. In Á. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New contributions in information systems and technologies* (Vol. 353, pp. 311–316). Springer. https://doi.org/10.1007/978-3-319-16486-1_31
- Bodeau, D., & Graubart, R. (2011). Cyber resiliency engineering framework (MTR110237). The MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf
- Böhme, R. (2010). Security metrics and security investment models. In I. Echizen, N. Kunihiro, & R. Sasaki (Eds.), *Advances in information and computer security* (pp. 10–24). Springer. https://doi.org/10.1007/978-3-642-16825-3_2
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management in SMEs. *Electronic Journal of Information Systems Evaluation*, 19(1), 22–32.
- Center for Internet Security. (2021). CIS Controls v8. Center for Internet Security. <https://www.cisecurity.org/controls/v8>
- Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, 1–27. <https://doi.org/10.1016/j.cose.2015.09.009>

- Coghlan, D., & Brannick, T. (2014). *Doing action research in your own organization* (4th ed.). SAGE Publications.
- Computer Science Teachers Association. (2017). CSTA K–12 computer science standards, revised 2017. <https://csteachers.org/k12standards/>
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98. <https://doi.org/10.1287/isre.1070.0160>
- Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9, 744. <https://doi.org/10.3389/fpsyg.2018.00744>
- Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, 5(1), tyz013. <https://doi.org/10.1093/cybsec/tyz013>
- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983–988. <https://doi.org/10.1016/j.cose.2012.08.004>
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. <https://doi.org/10.1145/581271.581274>
- Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy*, 10(2), 33–39. <https://doi.org/10.1109/MSP.2011.181>
- Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. John Wiley & Sons. <https://doi.org/10.1002/9781119162315>
- International Organization for Standardization, & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022). <https://www.iso.org/standard/27001>
- ISACA. (2018a). *COBIT 2019 framework: Governance and management objectives*. Information Systems Audit and Control Association.

- ISACA. (2018b). COBIT 2019 framework: Introduction and methodology. Information Systems Audit and Control Association.
- Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience*, 18(4), 277–290. <https://doi.org/10.12694/scpe.v18i4.1329>
- Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), 471–476. <https://doi.org/10.1007/s10669-013-9485-y>
- Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer. https://doi.org/10.1007/978-3-319-77492-3_1
- Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science*, 3(1/2), 81–98. <https://doi.org/10.1504/IJSSS.2011.038934>
- National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE Software*, 10(4), 18–27. <https://doi.org/10.1109/52.219617>
- Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). Workforce framework for cybersecurity (NICE Framework) (NIST SP 800-181r1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-181r1>
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597–611. <https://doi.org/10.1016/j.cose.2011.12.010>
- Reason, P., & Bradbury, H. (Eds.). (2008). *The SAGE handbook of action research: Participative inquiry and practice* (2nd ed.). SAGE Publications.

- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach (NIST SP 800-160, Vol. 2, Rev. 1). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-160v2r1>
- Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In L. F. Cranor & S. Garfinkel (Eds.), *Security and usability: Designing secure systems that people can use* (pp. 13–30). O'Reilly Media.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225. <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>
- Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CK: Design and philosophy (MP180360R1). The MITRE Corporation.
https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- West, R. (2008). The psychology of security. *Communications of the ACM*, 51(4), 34–40.
<https://doi.org/10.1145/1330311.1330320>