DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de integração de controles de segurança baseados nos princípios *Zero Trust* em uma *cyber supply chain*

Thiago Melo Stuckert do Amaral

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de integração de controles de segurança baseados nos princípios *Zero Trust* em uma *cyber supply chain*

Thiago Melo Stuckert do Amaral

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. João José Costa Gondim, FT/UnB _____
Orientador

Prof. Dr. Dino Macedo Amaral, Banco do Brasil _____
Examinador Externo

Prof. Dr. Robson de Oliveira Albuquerque, FT/UnB _____
Examinador Interno

PUBLICAÇÃO: PPEE.MP.030

FICHA CATALOGRÁFICA

AMARAL, THIAGO MELO STUCKERT DO
Proposta de integração de controles de segurança baseados nos princípios *Zero Trust* em uma *cyber supply chain* [Distrito Federal] 2022.
xvi, 76 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. *Cyber supply chain*	2. *Zero Trust*
3. *Software Bill of Materials* (SBOM)	4. DevSecOps
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

AMARAL, THIAGO M. S. (2022). *Proposta de integração de controles de segurança baseados nos princípios Zero Trust em uma cyber supply chain*. Dissertação de Mestrado Profissional, Publicação PPEE.MP.030, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 76 p.

CESSÃO DE DIREITOS

AUTOR: Thiago Melo Stuckert do Amaral
TÍTULO: Proposta de integração de controles de segurança baseados nos princípios *Zero Trust* em uma *cyber supply chain*.
GRAU: Mestre em Engenharia Elétrica ANO: 2022

Thiago Melo Stuckert do Amaral
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

AGRADECIMENTOS

Primeiramente, agradeço ao meu orientador Prof. Dr. João José Costa Gondim por todos os ensinamentos e conselhos durante essa jornada do mestrado profissional. A sua disposição em debater os mais diversos temas da área de segurança cibernética foi primordial para o desenvolvimento deste trabalho.

Também aproveito para agradecer toda a minha família e amigos. Em especial a minha mãe por ser a maior incentivadora dos meus estudos, pedra estrutural da minha educação e meu maior apoio. Ao meu pai por me encorajar a criar um sítio eletrônico com treze anos de idade. A minha avó Edila por ter despertado minha curiosidade para o campo das exatas por meio do exercício de sua profissão como professora de matemática. Bem como o papel fundamental de minha avó Rejane, que representou um porto seguro na minha infância. Aos meus avôs, anjos da guarda, Jair e Francisco. Além da importante participação na minha criação das minhas tias Ana Paula, Renata e Mariana, do meu "primo-irmão" Gabriel e do meu afilhado Luís Felipe. E demais tias avós, tios avôs, primas e primos que constituem uma parte essencial da grande família. Por fim, não posso deixar de mencionar o companheirismo da Júlia que nos últimos tempos me instigou a escalar montanhas e escrever artigos.

Esse trabalho foi parcialmente suportado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), pelo Sistema Brasileiro de Inteligência (SisBin), pelo Tribunal Superior Eleitoral (TSE) e pela Rede GigaCandanga.

RESUMO

A *cyber supply chain* tem sido alvo de ataques cada vez mais sofisticados que exploram vulnerabilidades em componentes que antes eram considerados seguros devido às relações de confiança existentes. Durante esse trabalho foi realizada uma ampla revisão dos controles de segurança de uma *cyber supply chain*. De forma a propor um conjunto mais abrangente de famílias de controles que os trabalhos correlatos identificados. A abordagem adotada revisa todas as relações de confiança. Desconsidera a confiança implícita em qualquer componente e baseia-se na premissa da existência de ameaças internas à rede corporativa. O presente trabalho propõe a integração de uma arquitetura *Zero Trust* em uma *cyber supply chain*. A principal contribuição deste estudo é propor uma organização de controles de segurança para uma *cyber supply chain* em domínios, permitindo melhorias de segurança por meio da aplicação de princípios de uma arquitetura *Zero Trust*. O estudo também fornece um *checklist* que permite uma análise de *gap* e sugere algumas formas de visualização desse resultado. Essas visualizações facilitam a construção de um *roadmap* de melhorias de segurança. E por último, são apresentados três estudos de caso aplicando a proposta em cenários de ataques reais ocorridos recentemente.

ABSTRACT

The cyber supply chain has been a target of sophisticated attacks. Vulnerabilities in components that were once considered secure due to perceived trusting relationships are being exploited. In the course of this work a comprehensive review of the security controls of a cyber supply chain was conducted. In order to propose a more comprehensive set of family controls than the related work identified. The adopted approach revises trust in all relationships. It disregards the implicit trust in any component and is based on the premise of the existence of internal threats to the corporate network. The present work proposes to integrate a Zero Trust architecture in a cyber supply chain. The main contribution of this study is to propose an organization of security controls for a cyber supply chain in domains, enabling improvements in the security of the cyber supply chain by applying the principles of a Zero Trust architecture. The study also provides a checklist of controls that allows a gap analysis and suggests some ways of visualizing this result. These visualizations provide an easy way to build a roadmap of security improvements. At last, it conducts three case studies applying the proposal to recent real-world attack scenarios.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES

ABIN	Agência Brasileira de Inteligência
APTs	*Advanced Persistent Threats*
BYOD	*Bring Your Own Device*
CIS	*Center of Internet Security*
CISA	*Cybersecurity and Infrastructure Security Agency*
CNCF	*Cloud Native Computing Foundation*
CSA	*Cloud security alliance*
CVE	*Common Vulnerabilities and Exposures*
CVSS	*Common Vulnerability Scoring System*
ENISA	*European Union Agency for Cybersecurity*
FBI	*Federal Bureau of Investigation*
FIPS	*Federal Information Processing Standard*
GDPR	*General Data Protection Regulation*
GOSST	*Google Open Source Security Team*
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IaC	*Infrastructure as code*
IETF	*Internet Engineering Task Force*
LGPD	Lei Geral de Proteção de Dados Pessoais
NCSC	*National Cyber Security Centre*
NIST	*National Institute of Standards and Technology*
OpenSSF	*Open Source Security Foundation*
OSINT	*Open Source Intelligence*
OWASP	*Open Web Application Security Project*
PNI	Política Nacional de Inteligência
Plansic	Plano Nacional de Segurança de Infraestruturas Críticas
SBOM	*Software Bill of Materials*
SCA	*Software Composition Analysis*
SCADA	*Supervisory Control And Data Acquisition*
SCIM	*Supply Chain Integrity Model*
SCITT	*Supply Chain Integrity, Transparency and Trust*
SisBin	Sistema Brasileiro de Inteligência
SLSA	*Supply chain Levels for Software Artifacts*
SOSR	*Secure Open Source Rewards*
SSDF	*Secure Software Development Framework*
TSE	Tribunal Superior Eleitoral
UEBA	*User and Entity Behavior Analytics*
WCNPS	*Workshop on Communication Networks and Power Systems*

1 INTRODUÇÃO

Os recentes ataques à *cyber supply chain* de infraestruturas críticas demostram a importância de se investir em controles de segurança para mitigar riscos dessa natureza [1]. O governo norte-americano já demonstrou sua preocupação com a segurança cibernética da *supply chain* por meio de algumas ordens executivas. Podemos definir a *cyber supply chain* como um ecossistema complexo e interconectado que engloba todo o ciclo de vida do *software*, *hardware* e serviços de um ampla variedade de entidades, incluindo vendedores, fornecedores, prestadores de serviço e contratados [2].

Uma ordem executiva norte-americana publicada em setembro de 2022 contém alguns guias para garantir que as agências federais somente usem *softwares* que sejam desenvolvidos seguindo boas práticas de segurança da informação [3]. Esse documento também cita uma série de invasões ao governo norte-americano nos últimos dois anos. Esses incidentes ameaçaram a prestação de serviços do governo norte-americano, além de comprometerem a integridade de uma imensa quantidade de informações pessoais e de dados sobre negócios administrados por empresas privadas.

Considerando esse cenário global de ameaças cibernéticas explorando vulnerabilidades na *cyber supply chain*, este trabalho apresenta algumas medidas de proteção que podem ser implementadas para melhorar a segurança da *cyber supply chain* em infraestruturas críticas. Uma das opções de mitigação de riscos dessa natureza é a adoção de boas práticas de uma arquitetura *Zero Trust*. Tal arquitetura refere-se a um modelo de segurança cibernética que assume que as ameaças existem tanto fora como dentro das fronteiras tradicionais de uma rede corporativa [4, 5]. Este modelo rejeita a confiança implícita em qualquer componente. Em vez disso, requer uma verificação explícita com monitoração constante da operação por meio de informações coletadas de múltiplas fontes em tempo real. Assim, a aplicação do *Zero Trust* é essencial, pois ao expor os riscos nas relações entre as partes interessadas, a organização é obrigada a rever os controles utilizados para aceitar e tratar os riscos existentes.

1.1 MOTIVAÇÃO

Existe uma tendência de aumento dos ataques utilizando vulnerabilidades presentes na *cyber supply chain*, conforme estudo realizado pela *European Union Agency for Cybersecurity* (ENISA) [6]. Uma das grandes vantagens desse tipo de abordagem é o seu amplo impacto. Por meio desse vetor de ataque é possível violar os mecanismos de proteção de uma grande quantidade de clientes de um *software*, ao comprometer o fornecedor de um componente comum a todos [6].

Um dos ataques recentes mais notórios ficou conhecido como "sunburst". Nesse incidente foram exploradas vulnerabilidades de um *software* de gerenciamento de redes fornecido pela empresa Solarwinds afetando diversas agências do governo norte-americano [7, 6]. Esse incidente demonstrou o potencial devastador da exploração de uma vulnerabilidade na *cyber supply chain*. Sendo avaliado pelo estudo da ENISA como um dos maiores ataques utilizando uma falha na *cyber supply chain* dos últimos anos, um dos

critérios utilizados para essa classificação foram os alvos atingidos, órgãos do governo norte-americano e grandes empresas privadas [6].

Considerando o problema exposto e a escassez de soluções, o presente trabalho apresenta uma proposta de integração de controles de segurança baseados nos princípios *Zero Trust* que pode ser aplicada na proteção de uma *cyber supply chain* de uma infraestrutura crítica.

1.2 OBJETIVOS

Esse trabalho foi formulado com o objetivo geral de propor uma integração de controles de segurança baseado em *Zero Trust* para mitigar riscos em uma *cyber supply chain*. E com os seguintes objetivos específicos:

- Revisar e comparar as famílias de controles implementadas pelos principais trabalhos correlatos identificados;
- Propor os controles baseados nas famílias de controles revisadas;
- Relacionar os princípios *Zero Trust* com os controles de segurança propostos;
- Classificar os controles em domínios temáticos e em estágios de implementação;
- Fornecer um *checklist* de implementação dos controles;
- Propor uma visualização da mensuração dos controles que auxilie o desenho de um *roadmap*;

1.3 CONTRIBUIÇÕES DO TRABALHO

A principal contribuição deste estudo é propor uma integração de controles de segurança baseados nos princípios *Zero Trust* em uma *cyber supply chain*. Essa proposta é organizada em domínios e estágios de forma a facilitar o seu entendimento e implementação. Este trabalho também visa proporcionar visibilidade aos riscos identificados na *cyber supply chain*. Além de permitir a construção de um *roadmap* para a adoção de controles baseados em uma abordagem baseada em princípios *Zero Trust*.

1.3.1 Publicação resultante desta pesquisa

Esta pesquisa teve como resultado a publicação do artigo *Integrating Zero Trust in the cyber supply chain security* [8] no *Workshop on Communication Networks and Power Systems* (WCNPS) em 2021.

1.4 ESTRUTURA DO TRABALHO

A dissertação a seguir está dividida em 5 capítulos, sendo este primeiro capítulo a introdução. O segundo capítulo apresenta o referencial teórico e os trabalhos correlatos. O terceiro capítulo detalha o modelo proposto para integração dos controles de segurança baseados em princípios *Zero Trust* para mitigar riscos de uma *cyber supply chain*. O quarto capítulo demonstra os cenários detalhados em três estudos de caso. E por fim, o último capítulo expõe algumas conclusões desse estudo e sugere trabalhos futuros.

2 DEFINIÇÕES CONCEITUAIS E TRABALHOS CORRELATOS

Este capítulo apresenta algumas definições conceituais sobre *cyber supply chain* e *Zero Trust*, além de detalhar trabalhos correlatos, normativos e ferramentas relacionadas aos assuntos explorados por este trabalho. Para facilitar o entendimento, o presente capítulo está organizado em seis tópicos maiores. Na Seção 2.1 é ilustrado o método de pesquisa de bibliografia adotado por esse estudo. Na Seção 2.2 são apresentados os conceitos que definem um ataque na *cyber supply chain*. A Seção 2.3 ilustra o conceito de *Software Bill of Materials* (SBOM). Já a Seção 2.4 detalha a definição conceitual de *Zero Trust* e elenca seus princípios. Na Seção 2.5 expõe alguns trabalhos relacionados, normativos de governos e ferramentas. E por fim, na seção 2.6 é detalhada a identificação da oportunidade de pesquisa.

2.1 MÉTODO DE PESQUISA

No levantamento da bibliografia relacionada foram utilizados o Portal de Periódicos da CAPES e o *Google Scholar*. Sendo que no Portal de Periódico da CAPES foi utilizada a base *Web of Science* - Coleção Principal. Também foram consultados os sítios eletrônicos de grandes fornecedores de soluções de tecnologia como o Google e Microsoft. Além de projetos de código aberto, como *Open Web Application Security Project* (OWASP), *Linux Foundation* e *Cloud Native Computing Foundation* (CNCF).

As buscas foram filtradas por meio das palavras-chave *cyber supply chain*, *software supply chain*, *Zero Trust*, *Software Composition Analysis* (SCA), *Solarwinds*,*Sunburst*, *Log4J* e *Colonial Pipeline*. E a combinação desses termos usando o operador lógico *AND*. Foram priorizados os artigos mais recentes. Além disso, a quantidade de citações foi considerada como indicador de impacto do estudo.

2.2 *CYBER SUPPLY CHAIN*

A *supply chain* refere-se ao ecosistema de processos, pessoas, organizações, e distribuidores envolvidos na criação e entrega de uma solução ou produto final [9]. No contexto da cibersegurança, a *cyber supply chain* abrange uma ampla variedade de recursos de *software* e *hardware*, armazenamento de dados (*cloud* ou local), mecanismos de distribuição de artefatos (aplicações *web*, lojas *online*) e armazenamento de artefatos de *software* [6].

Neste estudo preferimos o uso do termo *cyber supply chain* em detrimento de *software supply chain* pelo fato de o primeiro ser o empregado pelos normativos do governo norte-americano. Além disso, o termo *cyber* é mais abrangente do que apenas *software*. Todavia, não se observou uma uniformidade no entendimento das organizações de qual termo é mais apropriado durante a busca do referencial teórico. Percebe-se que algumas vezes os dois termos são usados como sinônimos.

Os ataques à *cyber supply chain* guardam algumas similaridades com os chamados *Advanced Persistent Threats* (APTs). Segundo o glossário do NIST, APT pode ser definido como um adversário com um nível sofisticado de conhecimento e quantidade significativa de recursos, permitindo que realize múltiplos vetores de ataques diferentes para gerar oportunidades de alcançar os seus objetivos, os quais são tipicamente estabelecer e aumentar sua presença dentro da infraestrutura de tecnologia de informação de uma organização com o propósito de continuamente extrair informações ou prejudicar o negócio da organização [10]. Essa definição se enquadra no comportamento de diversos ataques à *cyber supply chain* analisados pela ENISA, que na maioria das vezes são direcionados, complexos, custosos e planejados por um longo período de tempo.

2.3 *SOFTWARE BILL OF MATERIALS* (SBOM)

Os paradigmas de programação atuais encorajam a reutilização de componentes de *software* devido ao aumento de eficiência. Portanto, é comum que programadores criem soluções por meio da combinação de componentes de código aberto ou de código proprietário. O SBOM consiste num documento com os detalhes e relações da *cyber supply chain* de vários componentes utilizados na construção da solução. Esse artefato enumera os componentes de um produto de maneira a identificar sua versão e fornecedor, análogo a uma lista de ingredientes de um produto alimentício [11].

Esse detalhamento também pode ser útil na identificação de vulnerabilidades recentemente descobertas em componentes desenvolvidos por terceiros, sendo importante uma padronização do formato do SBOM para facilitar a leitura e utilização dessas informações [12], assim permitindo a automação da sua análise e a incorporação num ciclo de desenvolvimento seguro. Esse tipo de esteira de desenvolvimento é conhecido como *pipeline* DevSecOps, pois considera aspectos das atividades de operação de tecnologia e segurança cibernética. Outra medida interessante é a centralização dessa informação para que se possa construir um painel de monitoramento desses riscos.

2.3.1 Ferramentas de análise de dependências

Algumas ferramentas implementam parte das necessidades descritas acima. Pode-se destacar o software de código aberto *dependency track* desenvolvido pela comunidade da *Open Web Application Security Project* (OWASP).

Esse utilitário é integrado em um *pipeline* para monitorar as bibliotecas de código aberto que já possuem vulnerabilidades publicadas no banco de dados *Common Vulnerabilities and Exposures* (CVE) [13].

No entanto, essa ferramenta não é capaz de analisar como as vulnerabilidades dos componentes podem ser transmitidas para o produto final e também não analisa a aderência às boas práticas de uma arquitetura *Zero Trust*, tópicos abordados pelo presente estudo.

Outra ferramenta de código aberto é a Pyrsia [14] que auxília na proteção da *supply chain* por ser uma rede descentralizada de pacotes que permite aos desenvolvedores baixarem as dependências de maneira segura e transparente. Os pacotes são assinados garantindo a autenticidade e integridade do código, além

da propriedade de não-repúdio , também conhecido como o princípio da irretratabilidade.

Outra plataforma importante é a deps.dev desenvolvida pelo Google que permite realizar algumas análises de dependências vulneráveis verificando as relações entre projetos de código aberto [15]. A plataforma monitora constantemente alguns repositórios de código aberto como, por exemplo, <github.com>, <npmjs.com> e <pkg.go.dev> em busca de informações atualizadas sobre os pacotes. A partir dessa informação, a plataforma cria um grafo de dependências completo, representando até dependências transitivas, ou seja, as dependências das dependências. Esse grafo proporciona mais transparência na *supply chain*, permitindo uma maior visibilidade de quais componentes de softwares são afetados quando ocorre algum problema em um pacote de código aberto.

A empresa Synopsys produziu um relatório sobre como os projetos de desenvolvimento de software são dependentes de bibliotecas de código aberto [16]. Na figura 2.1 são apresentadas algumas estatísticas dos projetos analisados.

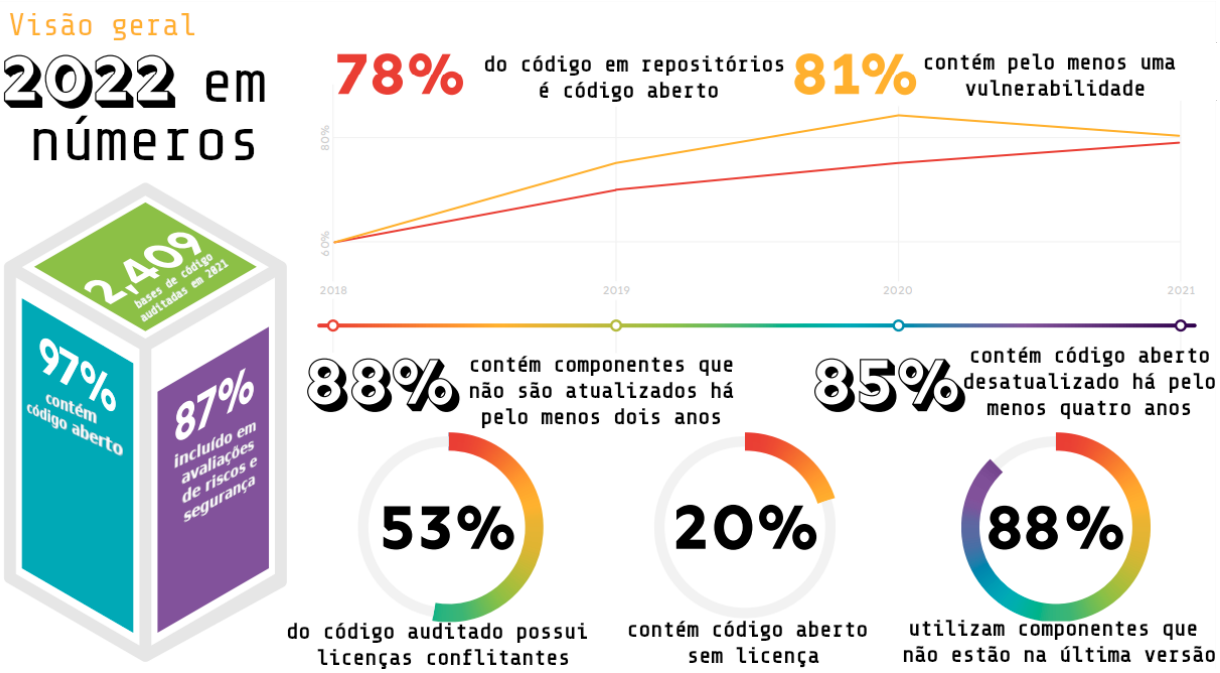

Figura 2.1: Estatísticas de estudo da Synopsys sobre projetos *opensource*. Adaptado do relatório da Synopsys [16].

Os membros da *Open Source Security Foundation* (OpenSSF) criaram um projeto para atribuir uma pontuação de criticidade em projetos de código aberto [17]. Um dos objetivos do projeto é criar uma lista dos projetos críticos que a comunidade de código aberto utiliza. E com essas informações aprimorar proativamente a segurança desses projetos. Também existe outro projeto da OpenSSF que avalia projetos de código aberto por meio de métricas de qualidade [18].

A fundação do Linux criou um programa de recompensas chamado *Secure Open Source Rewards* (SOSR). Esse programa apoia financeiramente desenvolvedores que contribuem com melhorias de segurança em projetos críticos de código aberto [19]. Esse projeto é patrocinado pelo *Google Open Source Security Team* (GOSST).

2.4 DEFINIÇÃO CONCEITUAL DO MODELO *ZERO TRUST*

A transformação digital acelerada pela pandemia de COVID-19 promoveu o trabalho remoto e outras interações digitais. Nesse cenário, um modelo de proteção baseado em perímetros, segmentação da rede em sub-redes, não é suficiente para enfrentar os problemas atuais[20]. Outro ponto importante a se destacado é o aumento de ameaças internas à organização. Agentes internos e dispositivos supostamente confiáveis se tornaram vetores de ataques. Além disso, a política *Bring Your Own Device* (BYOD) de utilizar dispositivos pessoais no trabalho é um desafio para o modelo baseado em perímetros. Nesse contexto, o estudo [21] revisa os problemas de segurança da informação deste modelo e aponta possíveis temas para pesquisas futuras. Adicionalmente, as organizações estão cada vez mais adotando um paradigma de computação em nuvem para ganhar escala, diminuir custos e aumentar a mobilidade. Cabe destacar que novas pequenas empresas do ramo financeiro, conhecidas como *fintechs*, já nascem nesse contexto de nuvem e precisam precisam enfrentar desafios relacionados à confiança em ambientes administrados por terceiros desse paradigma. Com o intuito de lidar com esses desafios, o trabalho [22] explora como uma estratégia conceitual de mecanismos de segurança baseados num modelo *Zero Trust* pode proteger um ambiente de computação na nuvem.

O conceito de *Zero Trust* já era presente em algumas estratégias de proteção antes mesmo do conceito existir. Por exemplo, as agências norte-americanas *Defense Information Systems Agency* (DISA) e *Department of Defense* (DoD) já haviam publicado documentos sobre a proteção de organizações usando uma estratégia chamada *black core*, que se baseava na proteção de transações individuais [23].

Um dos primeiros trabalhos acadêmicos que definiu em 1994 o conceito de *Zero Trust* foi a tese de doutorado de Stephen Paul Marsh da Universidade de Stirling, que apresenta um formalismo matemático sobre confiança [24]. Em 2003, o modelo *Zero Trust* ficou popular no fórum Jericho, posteriormente esse fórum se transformou no *The Open Group Security Forum* [25]. Esse modelo é uma quebra do paradigma de segurança baseada em perímetro, no qual os ativos da organização são considerados seguros por estarem dentro de um ambiente segregado da internet. Essa divisão dos ambientes é costumeiramente realizada por meio de equipamentos de segurança como *firewalls*, *Intrusion Detection Systems* (IDS) e *Intrusion Prevention Systems* (IPS). Já nesse novo modelo os ativos da organização são protegidos independente da sua localização, conforme figura 2.2.

Como fonte do referencial teórico também podemos destacar o grupo de trabalho da *Cloud security alliance* (CSA). Esse grupo de trabalho produziu documentos com algumas perspectivas sobre *Zero Trust* de gestores na área de segurança cibernética e relatos sobre o progresso na implantação de *Zero Trust* em suas organizações [26].

É interessante apresentar uma declaração de Eric Goldstein, diretor executivo assistente da CISA, em um pronunciamento sobre prevenção e resposta a ataques *ransomwares* no Senado norte-americano [27]. Nessa declaração Goldstein afirmou que a CISA está investindo em aumentar sua capacidade em melhorar a visibilidade dos riscos de segurança cibernéticos nas agências federais. Com esse intuito, estão aperfeiçoando suas habilidades em conduzir investigações em buscas de ameaças (*threat hunting*), coleta e análise de dados de segurança em todos os níveis da rede, e análises rápidas para identificar e se proteger de ameaças conhecidas. Essa primeira parte do pronunciamento demonstra a importância da gestão dos riscos

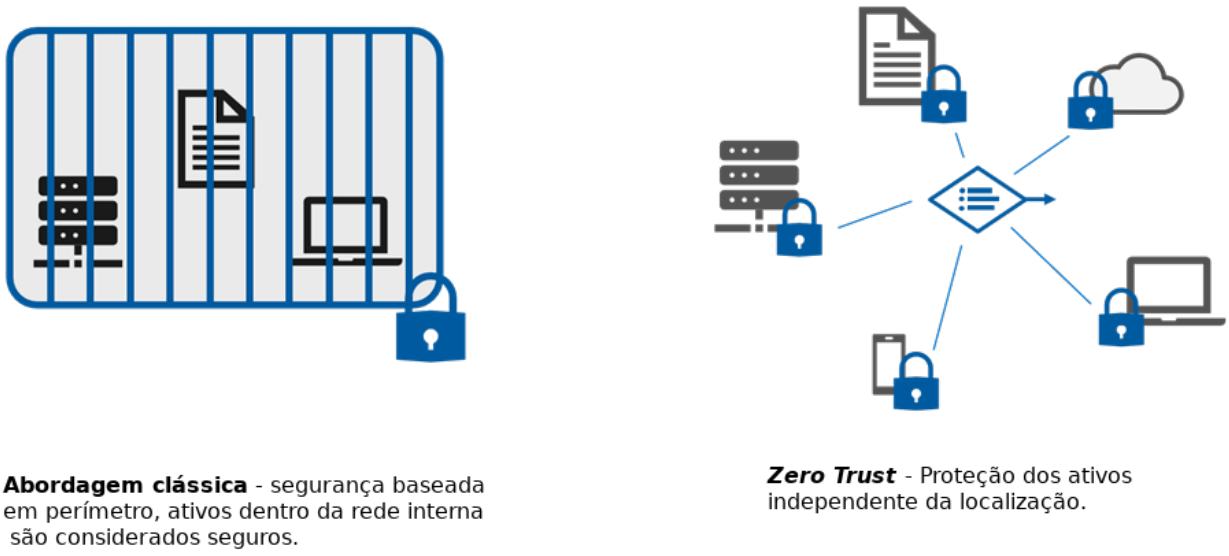

Figura 2.2: Diferença da abordagem clássica e do modelo *Zero Trust*. Ilustração adaptada da documentação da Microsoft [25].

de segurança cibernéticos e da área de ciência de dados capaz de fornecer técnicas e ferramentas para a condução dessas análises e apoiar a tomada de decisão tempestiva para proteger as infraestruturas críticas.

Na segunda parte do pronunciamento, Goldstein explica que existe uma série de iniciativas para se adotar uma arquitetura de redes defensiva com adoção da abordagem *Zero Trust*, modelo de arquitetura utilizado como base para a proposta de integração apresentada neste trabalho [27]. E por fim, Goldstein ressalta a importância da colaboração de várias entidades do governo e da iniciativa privada para a efetiva proteção das infraestruturas críticas.

2.4.1 Princípios *Zero Trust*

Um dos princípios fundamentais de uma arquitetura *Zero Trust* é autorizar toda comunicação segura entre os recursos, independente do ambiente e da localização, e ter como premissa básica que toda comunicação de rede é uma fonte de ameaça até que seja verificada, autorizada e protegida [28].

Isso não é meramente uma extensão dos princípios de segurança de negar por padrão, menor privilégio, e controle de acesso baseado em papéis. Em vez disso, é uma redefinição da abordagem *ring-fence*, que presume uma barreira virtual que separa o ambiente interno da organização dos demais ativos ligados na *internet*. Na abordagem *Zero Trust*, os recursos são protegidos individualmente, essa técnica também é conhecida como microsegmentação. O objetivo da microsegmentação é isolar o tráfego de cada segmento para um melhor controle e monitoração. A implementação da microsegmentação reduz a superfície de ataque para um mínimo viável e bloqueia qualquer movimento lateral não autorizado. As solicitações de acesso não autorizada são bloqueadas e colocadas em quarentena, e os alertas são escalados para que novos dados de inteligência de ameaça sejam investigados [29].

O escopo dos controles de segurança cibernética não são mais limitados ao perímetro de rede. Dado que o novo paradigma de plataformas de nuvem e trabalho remoto adicionaram mais desafios para o time

de segurança gerenciar a infraestrutura da organização e proteger seus dados valiosos. Portanto, uma medida de salvaguarda da infraestrutura e dos dados é crítica para o sucesso das operações de negócio da organização.

O sucesso de uma microsegmentação baseada nos princípios *Zero Trust* depende da proteção do tráfego da rede e de seus dados. Dessa forma, essa boa prática tem como objetivo realizar um filtro granular do que é possível proteger com os segmentos [29]. Outro princípio importante de segurança cibernética é a segregação de deveres. Esse princípio garante que o mesmo usuário não possui permissões para executar atividades que quando combinadas implicam em riscos elevados. Essa abordagem é amplamente citada na literatura para mitigar riscos em infraestruturas críticas [30].

2.5 TRABALHOS RELACIONADOS

O presente trabalho é uma evolução das questões acadêmicas sugeridas por Z. A. Collier e J. Sarkis [31], nesse estudo é sugerida a integração dos princípios *Zero Trust* na construção de mecanismos de proteção de uma *cyber supply chain*, no entanto não fornece os detalhes. A evolução desse estudo aqui apresentada é uma proposta de *checklist* de controles relacionados com a *cyber supply chain* e visualizações dos resultados obtidos.

Outro estudo que também inspirou o presente trabalho é o artigo escrito por Pratim Datta [7], que exalta a importância de se combater ataques na *cyber supply chain*. No entanto, não esclarece como seriam implementados esses mecanismos de proteção, tema explorado no presente trabalho.

A proposta de integração aqui apresentada baseou-se nos princípios de *Zero Trust* estabelecidos pelo *National Institute of Standards and Technology* (NIST) na publicação especial *Sp 800-207 - Zero Trust architecture* [23]. Também utilizou as categorias de controles apresentados no guia NIST *Cyber supply chain risk management practices for systems and organizations* [32]. Estes elementos foram integrados de forma semelhante ao demonstrado no modelo *Zero Trust Maturity Model* da *Cybersecurity and Infrastructure Security Agency* (CISA)[33].

Outro estudo relacionado com este trabalho foi conduzido por Abhijeet Ghadge, Maximilian Weiß, Nigel D. Caldwell, Richard Wilding, em [34], o qual investiga a gestão de riscos cibernéticos no contexto da *cyber supply chain*. E por último, o estudo conduzido por Abel Yeboah-Ofori e Shareeful Islam, em [35], serviu de fonte de inspiração para os controles propostos de uma *cyber supply chain*.

O *framework* do Mitre detalha uma técnica com o nome "comprometimento da *supply chain*", porém não realiza um estudo aprofundado de como são conduzidos esses ataques [36]. O trabalho realizado por Qiushi Wu e Kangjie Lu analisa como poderiam ser inseridas vulnerabilidades no kernel do linux por meio da inserção de código malicioso proveniente de uma contribuição para o projeto *open source*[37]. O estudo feito por Topping C., Michalee O., e Rashid A. [38] faz uma comparação de algumas abordagens para identificar e gerenciar riscos da *cyber supply chain*.

2.5.1 Normativos do governo brasileiro

Em âmbito local, o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC) cita que ações de inteligência de Estado devem monitorar constantemente as ameaças [39]. E essas ações podem eventualmente indicar a necessidade de ajustes nos sistemas de proteção das infraestruturas críticas nacionais. Com a finalidade de executar esse monitoramento, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) conta com o apoio da Agência Brasileira de Inteligência (ABIN). De acordo com o disposto no inciso III do *caput* do art. 4º da lei de criação da ABIN [40], uma das competências da Agência é "avaliar as ameaças, internas e externas, à ordem constitucional", o que inclui ameaças à segurança cibernética das infraestruturas críticas nacionais, algumas delas elencadas na Política Nacional de Inteligência (PNI) [41].

2.5.2 Normativos de governos estrangeiros

Durante a pesquisa do referencial teórico foram encontrados alguns normativos de governos estrangeiros. Dando destaque nessa seção para os documentos publicados pelo governo britânico e norte-americano.

2.5.2.1 Governo britânico

O *National Cyber Security Centre* (NCSC) do governo britânico publicou um guia de avaliação da segurança da *cyber supply chain* contendo cinco etapas[42]. De maneira simplificada as etapas sugeridas e suas atividades principais são:

- Análise inicial - identificação dos fornecedores e de como a organização trata os riscos atuais;
- Desenvolvimento de uma abordagem de avaliação - Determina os ativos críticos e prioriza os controles a serem implementados;
- Aplica a abordagem nas novas relações com os fornecedores - Conscientiza as equipes envolvidas e implementa os controles durante a duração do contrato;
- Integra a abordagem com as relações com os fornecedores existentes - Identifica os contratos atuais e revisa as cláusulas contratuais;
- Melhoria contínua - Avalia as abordagens e os componentes regularmente, além de atualizar os controles de acordo com as boas práticas atuais;

Existem algumas atividades que são executadas em mais de uma etapa, como, por exemplo, o monitoramento da segurança dos fornecedores e o envio de um relatório de progresso para um conselho administrativo da empresa.

2.5.2.2 Governo norte-americano

O memorando identificado pela sigla M-22-18 do governo norte-americano versa sobre como melhorar a segurança da *cyber supply chain* por meio da adoção de práticas de desenvolvimento seguro[43].

Esse documento menciona a ordem executiva sobre melhorias na cibersegurança nacional focando na segurança e integridade da *cyber supply chain* e enaltece a importância de um ambiente de desenvolvimento seguro[44]. Esse normativo utiliza como base alguns padrões estabelecidos pelo NIST, como a *Special Publication* 800-218 - *Secure Software Development Framework* (SSDF) [45] e o guia *Software Supply Chain Security Guidance* [46].

Outro normativo importante para esse trabalho é a publicação especial do NIST 800-161 [32] que versa sobre as práticas de gerenciamento de riscos da *cyber supply chain*. Esse documento apresenta um processo sistemático de gerenciamento de riscos da *cyber supply chain* por meio dos instrumentos adequados. O intuito desse documento é apresentar um guia que permita identificar, avaliar, selecionar e implementar controles capazes de mitigar riscos de segurança na *cyber supply chain*. Na seção 2.6.1 são detalhadas as famílias de controles utilizadas nesse trabalho.

O governo norte-americano também definiu os elementos mínimos de um SBOM no documento[47] em decorrência da ordem executiva 14028 sobre melhorias na cibersegurança [44]. Essa ordem executiva enaltece a importância de se manter o SBOM atualizado com informações precisas sobre a origem dos componentes de *software*. E também sugere que devem ser implementados controles sob os componentes de terceiros, as ferramentas e serviços utilizados durante o processo de desenvolvimento. Além de recomendar auditorias frequentes para verificar se os controles estão sendo executados. Já em âmbito nacional, um exemplo de lista de dependências divulgada pelo governo brasileiro é o rol de bibliotecas utilizadas pela justiça eleitoral. O Tribunal Superior Eleitoral (TSE) divulga os *hashes* de todos os arquivos utilizados na urna eletrônica no seu sítio eletrônico oficial [48]. Apenas para exemplificar, pelo site do TSE é possível obter a informação que o sistema "pc1TRAN" utiliza a biblioteca "log4j" na versão "1.2.17".

2.5.3 Relatório da *European Union Agency for Cybersecurity* (ENISA)

O estudo da ENISA elenca quatro elementos de uma *supply chain*[6]:

- Fornecedores: são organizações que fornecem um produto ou serviço para outra organização;
- Ativos fornecidos: são elementos valiosos usados para produzir o serviço ou produto;
- Cliente: é a organização que consome o produto ou serviço produzido por um fornecedor;
- Ativos dos clientes: são elementos valiosos de propriedade do alvo.

Um ataque à *cyber supply chain* é a combinação de pelo menos dois ataques. O primeiro ataque é ao fornecedor que então é usado para atacar o alvo e ganhar acesso ao ativo. O alvo pode ser o cliente final ou outro fornecedor. Portanto, para que seja classificado como um ataque à *cyber supply chain*, é necessário que tanto o fornecedor quanto o cliente sejam alvos [6].

O estudo da ENISA propõe uma taxonomia para os ataques à *cyber supply chain*. Essa taxonomia facilita a comparação de alguns ataques e também pode ser um guia para a identificação de novos potenciais ataques. Essa taxonomia é representada pela tabela 2.1. Cabe observar que os autores do relatório da ENISA consideraram *Open Source Intelligence* (OSINT) uma técnica de ataque para comprometer a *supply chain*, porém não existe uniformidade na literatura sobre OSINT possuir essa finalidade.

A taxonomia é utilizada para identificar "como" o fornecedor foi atacado. E "qual" foi o alvo do ataque no lado do fornecedor. Já no aspecto do cliente, é identificado "como" o cliente foi atacado. E "o que" foi atacado no lado do cliente. Os ativos do fornecedor visados pelos atacantes referem-se a qual era o alvo do ataque à *cyber supply chain*, que permitiu a posterior condução de novos ataques.

Tabela 2.1: Proposta de taxonomia adaptada do relatório da ENISA [6].

Fornecedor		**Cliente**	
Técnica de ataque utilizada para comprometer a *supply chain*	Ativo do fornecedor visado pelo ataque	Técnica de ataque utilizada para comprometer o cliente	Ativo do cliente visado pelo ataque
Infecção por código malicioso	Código pré-existente	Relação de confiança	Dados
Engenharia social	Bibliotecas de software	*Drive-by Compromise*	Dados pessoais
Ataque força bruta	Código	*Phishing*	Propriedade intelectual
Exploração de vulnerabilidade de *software*	Configurações	Infecção por código malicioso	*Software*
Exploração por vulnerabilidade em uma configuração	Dados	Ataque físico ou modificação	Processos
Open Source Intelligence (OSINT)*	Processos	Falsificação	Largura de banda
	Hardware		Finanças
	Pessoas		Pessoas
	Fornecedores		

Vários vetores de ataques de comprometimento da *cyber supply chain* se mantém desconhecidos. O relatório da ENISA mostra que em 66% dos ataques analisados os fornecedores desconheciam a forma como tinha sido comprometidos. No entanto, menos do que 9% dos clientes comprometidos por meio de ataques à *cyber supply chain* não sabiam como os ataques haviam ocorrido. Esse fato demonstra a diferença de maturidade em relação aos incidentes de segurança cibernética relatados entre os fornecedores e os clientes finais. Considerando que 83% dos fornecedores são do setor de tecnologia, essa falta de conhecimento sobre como os ataques ocorrem representa um baixo grau de maturidade em cibersegurança ou uma política de falta de transparência no compartilhamento de informações. Existem também outros fatores que podem contribuir com a falta de entendimento sobre como os fornecedores são comprometidos, incluindo a complexidade dos ataques e a lentidão na descoberta dos ataques que podem dificultar a investigação.

O relatório da ENISA enumerou uma série de ataques apresentados nas tabelas 2.2 e 2.3. E por fim, a figura 2.3 apresenta uma linha do tempo dos ataques recentes à *cyber supply chain*.

2.5.4 *Supply chain Levels for Software Artifacts* (SLSA)

Outras iniciativas também abordam a segurança da *cyber supply chain*. O Google possui uma iniciativa chamada *Supply chain Levels for Software Artifacts* (SLSA) [49], que apresenta um conjunto de controles e recomendações cujo objetivo é garantir a integridade de cada elo de uma *cyber supply chain*. A SLSA foi

Tabela 2.2: Primeira parte da lista de ativos e organizações comprometidas por ataques na *supply chain*. Tabela adaptada a partir de [6].

Ativos e organizações	Técnica de ataque utilizada para comprometer a supply chain	Ativo do fornecedor visado pelo ataque	Técnica de ataque utilizada para comprometer o cliente	Ativo do cliente visado pelo ataque
Software de gerenciamento da KASEYA	Infecção por código malicioso	Código pré-existente	Relação de confiança, Infecção por código malicioso	Dados, Finanças
Solução de vigilância da VERKADA	OSINT	Configurações, Dados	Relação de confiança	Dados
Gerenciamento de códigos e soluções de auditoria da CODECOV	Exploração por vulnerabilidade em uma configuração	Código	Relação de confiança	Software
Programa de instalação da WIZVERA VERAPORT	Desconhecida	Processos	Drive-by Compromise, Infecção por código malicioso	Dados
Software de bate-papo da ABLE DESKTOP	Desconhecida	Código	Relação de confiança, Infecção por código malicioso	Dados
Software fiscal inteligente da AISINO	Desconhecida	Código	Relação de confiança, Infecção por código malicioso	Desconhecido
Emulador de android da BIGNOX NOXPLAYER	Desconhecida	Código	Relação de confiança, Infecção por código malicioso	Pessoas, Dados
Autoridade certificadora do governo do Vietnã	Desconhecida	Código	Relação de confiança, Infecção por código malicioso	Pessoas
Plataforma de desenvolvimento da APACHE NETBEANS	Infecção por código malicioso	Código	Infecção por código malicioso	Software, Dados
Gerenciador de senhas PASSWORDSTATE da CLICKSTUDIOS	Desconhecida	Código	Relação de confiança, Infecção por código malicioso	Dados
XCODE, ambiente de desenvolvimento integrado da APPLE	Desconhecida	Código	Infecção por código malicioso	Desconhecido

Tabela 2.3: Segunda parte da lista de ativos e organizações comprometidas por ataques na *supply chain*. Tabela adaptada a partir de [6].

Ativos e organizações	Técnica de ataque utilizada para comprometer a supply chain	Ativo do fornecedor visado pelo ataque	Técnica de ataque utilizada para comprometer o cliente	Ativo do cliente visado pelo ataque
Site presidencial de Myanmar	Desconhecida	Código	Phishing, Infecção por código malicioso	Pessoas
ORION, gerenciamento e monitoramento remoto da SOLARWINDS	Exploração de vulnerabilidade de software, Ataque força bruta, Engenharia social	Processos, Código	Relação de confiança, Infecção por código malicioso	Dados
Sistema de interação eletrônica dos órgãos executivos da Ucrânia	Desconhecida	Código	Infecção por código malicioso	Pessoas, Dados
Serviços de segurança cibernética na nuvem da MIMECAST	Desconhecida	Dados	Relação de confiança	Dados
Software de transferência de arquivos da ACCELLION	Exploração de vulnerabilidade de software	Código	Relação de confiança	Dados
Sistema de serviço de passageiros da SITA	Desconhecida	Dados	Desconhecida	Dados pessoais
Carteira de hardware da LEDGER	Desconhecida	Dados	Relação de confiança, Phishing, Falsificação	Finanças
Software de colaboração e gerenciamento de projetos da FUJITSU PROJECTWEB	Desconhecida	Código, Dados	Desconhecida	Dados
Sistema de comunicação de telefones celulares da UNIMAX	Desconhecida	Código	Relação de confiança, Infecção por código malicioso	Pessoas
Programa de compatibilidade de hardware com o Windows da Microsoft	Engenharia social	Processos	Relação de confiança	Dados
Autoridade certificadora da MONPASS	Exploração de vulnerabilidade de software	Código	Drive-by Compromise, Infecção por código malicioso	Desconhecido
Sistema para empresa de projeto e distribuição da SYNNEX IT	Exploração de vulnerabilidade de software	Código	Drive-by Compromise, Infecção por código malicioso	Desconhecido

projetada para ser independente de tecnologia e servir como uma linha de base de controles de segurança que podem ser aplicados em um componente de *software*.

A SLSA define quatro níveis, sendo que o primeiro nível é o de mais fácil adoção. Enquanto o quarto nível provê garantias de segurança mais robustas. No primeiro nível, a *cyber supply chain* está documentada e existe uma infraestrutura capaz de garantir a procedência dos artefatos. O segundo nível apresenta maior confiabilidade no processo de compilação e são utilizadas assinaturas digitais para evitar a adultera-

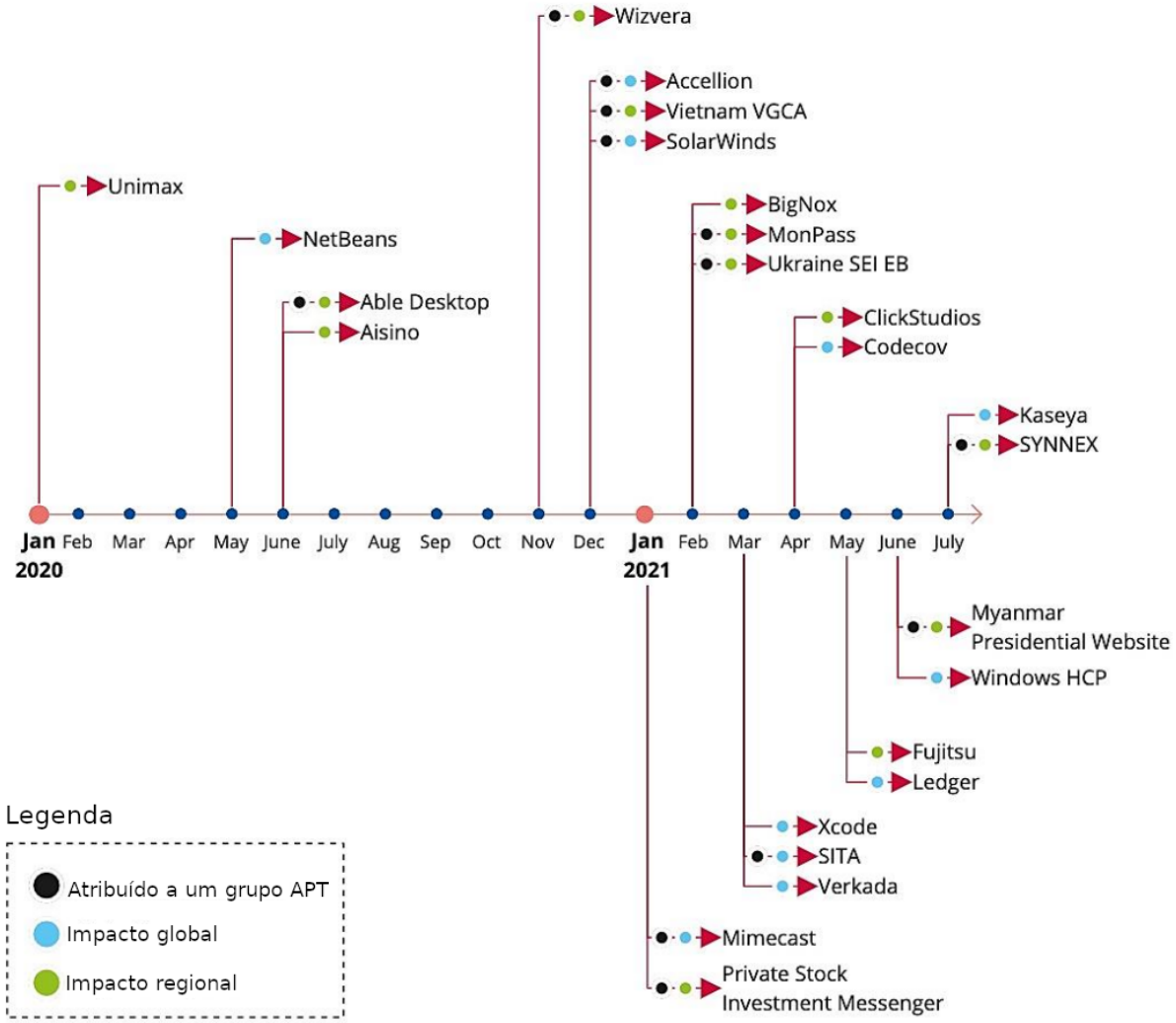

Figura 2.3: Linha do tempo de ataques recentes à *cyber supply chain*. Adaptado do relatório da ENISA [6].

ção da procedência dos artefatos. No terceiro nível, a compilação é digna de confiança e os parâmetros de compilação são definidos em código, além da integração contínua ser mais robusta. Por fim, no último nível o processo de compilação é rastreável, é possível verificar a autenticidade e integridade das dependências e as ameaças internas são mitigadas. Cabe destacar que a procedência é um metadado que demonstra como os artefatos foram compilados, isso inclui um detalhamento do processo, do código-fonte e de suas dependências. Cabe observar que os níveis do SLSA são medidos individualmente para cada artefato permitindo uma adoção gradual baseada em critérios de risco. A tabela 2.4 resume a descrição desses níveis.

A iniciativa SLSA foi projetada para ser capaz de apresentar provas verificáveis que um controle específico foi implementado na *cyber supply chain*. As provas verificáveis da SLSA podem utilizar o formato definido pela especificação *in-toto* [51]. Essa especificação garante que é possível verificar em cada etapa da *cyber supply chain* se a ação foi de fato realizada pela pessoa que possuía autorização para tal, e também é capaz de atestar modificações no componente durante essa etapa [51].

Um ataque à integridade de um componente de *software* pode ser realizada nas etapas de codificação, teste, compilação (*build*) e distribuição. Essas etapas são representadas na figura 2.4 adaptada da documen-

Tabela 2.4: Os níveis de segurança definidos pela SLSA. Adaptado da documentação do Google [50].

Nível	Descrição
0	Sem controles implementados.
1	O processo de compilação é automatizado. Também é possível verificar a procedência dos artefatos.
2	O controle de versão é obrigatório. Além disso, processo de compilação garante a autenticidade da procedência dos artefatos.
3	A plataforma de versionamento garante a rastreabilidade do código. E o processo de compilação garante a integridade dos artefatos.
4	Qualquer modificação é revisada por pelo menos dois membros da equipe (princípio da segregação de deveres). Além de ser possível reproduzir o processo de compilação.

tação do Google. Cabe destacar que os principais pontos de atenção no SLSA é a automação da entrega dos artefatos de *software* e a verificação das dependências.

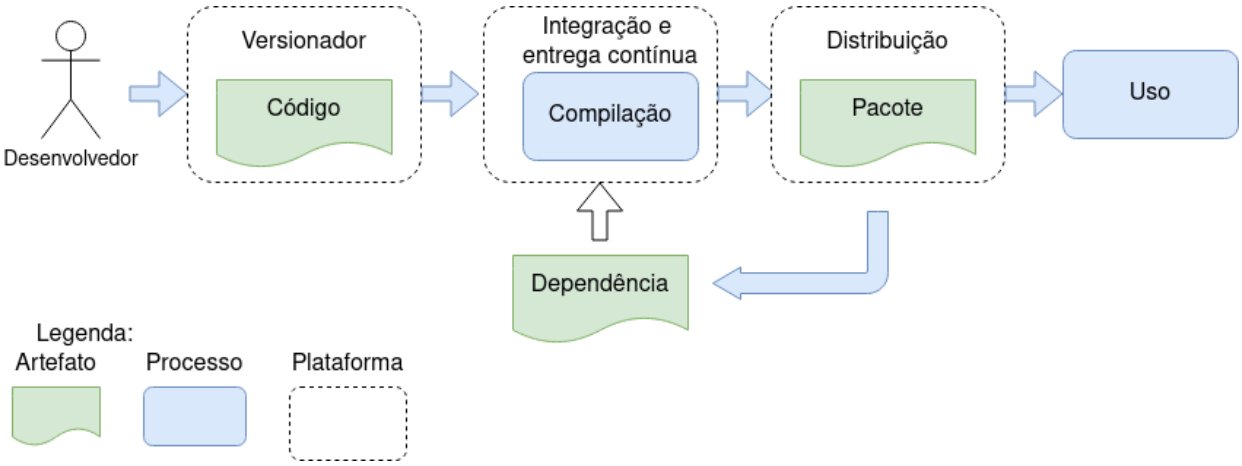

Figura 2.4: Etapas analisadas pela SLSA. Adaptado da documentação do Google [49].

A SLSA ilustra na figura 2.5, as principais ameaças cibernéticas presentes nas etapas representadas por 2.4. Cabe destacar que a SLSA estabelece três "plataformas" que são fronteiras de confiança representadas como caixas pontilhadas. Já os processos são desenhados por caixas azuis, e os artefatos são verdes. E por fim, as ameaças são simbolizadas por triângulos amarelos.

Destaca-se que as ameaças são separadas em dois tipos: integridade do código e integridade da compilação. Quanto à integridade do código, todo o código-fonte deve refletir a intenção do desenvolvedor, esse código e o histórico de alterações devem permanecer disponíveis para investigação. Uma integridade de código mais rigorosa significa melhor proteção contra código malicioso submetido sem revisão ou por um versionador comprometido. Já a integridade da compilação garante que o componente de software é construído a partir dos códigos e dependências corretos, que não sofrerem interferências indevidas. Um processo de compilação mais resiliente significa proteger os códigos contra modificações após serem versionados, uma plataforma de compilação não-comprometida, e garantir que não é possível deixar de utilizar a plataforma de integração e entrega contínua corporativa.

A SLSA incentiva a utilização de boas práticas de segurança para que sejam implementados os controles técnicos adequados. Alguns dos controles detalhados pela SLSA são a capacidade de analisar automaticamente artefatos, garantir a autenticidade e integridade do código, proteger contra modificações que

possam ocorrer nos processos de compilação e distribuição, isolar quaisquer vulnerabilidades ocultas e ser capaz de rastrear os componentes afetados.

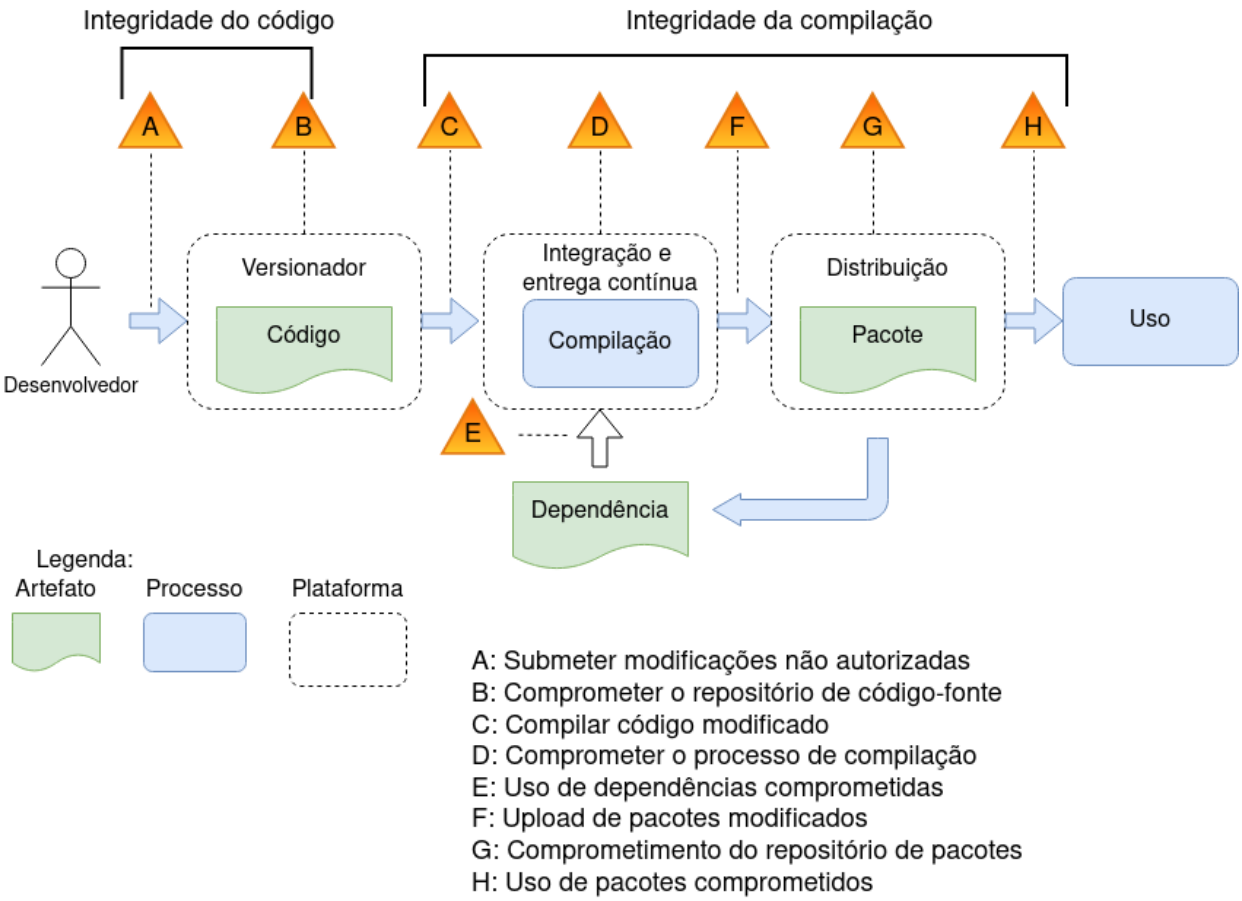

Figura 2.5: Ameaças identificadas pela SLSA. Adaptado da documentação do Google [52].

2.5.5 *Supply Chain Integrity, Transparency and Trust* (SCITT)

A Microsoft também tem teve uma iniciativa semelhante à SLSA chamada *Supply Chain Integrity Model* (SCIM) [53] que evoluiu para a *Supply Chain Integrity, Transparency and Trust* (SCITT). A SCITT é uma iniciativa da *Internet Engineering Task Force* (IETF) para criação de um conjunto de padrões para a indústria que tratem da conformidade dos componentes de uma *supply chain*. Esses padrões serão capaz de estabelecer a forma como esses componentes serão autenticados, e como ações sobre essas entidades serão autorizadas e auditadas [54].

Pelo fato dessa iniciativa ser muito recente e ter pouca documentação disponível foi excluída do rol de trabalhos correlatos a serem utilizados como base para a identificação da oportunidade de pesquisa deste trabalho.

2.5.6 *OWASP Top 10 CI/CD Security Risks*

A OWASP possui um projeto entitulado *OWASP Top 10 CI/CD Security Risks* que correspodem aos dez maiores riscos de um processo de integração e entrega contínua [55]. Os riscos listados nesse *rank* são:

- Controle insuficiente dos mecanismos de fluxo;
- Gerenciamento inadequado de identidade e acesso;
- Abuso na cadeia de dependências;
- Envenenamento do *pipeline* de execução;
- Controle insuficiente do acesso no *pipeline*;
- Higienização insuficiente das credenciais;
- Configuração insegura do sistema;
- Uso descontrolado de *plugins* de terceiros;
- Validação inapropriada da integridade dos artefatos;
- Visibilidade e *logs* insuficientes.

2.5.6.1 Processo de compilação hermético

O processo de compilação fechado (hermético) visa garantir a consistência dos artefatos e a repetibilidade do processo [56]. Caso dois desenvolvedores desejem construir a partir do repositório de código-fonte o mesmo produto com a versão igual em máquinas diferentes, é esperado que obtenham os mesmos resultados. O processo de compilação fechado é independente das bibliotecas ou outros *softwares* instalados na máquina de *build*. Nesse caso, o processo de compilação é autocontido e não deve depender de serviços externos ao ambiente de construção.

2.5.7 Guia de segurança da *software supply chain* do *Center of Internet Security* (CIS)

O *Center of Internet Security* (CIS) publicou em junho de 2022 um guia de segurança da *software supply chain* [57]. Esse guia é bem abrangente apresentando controles relacionados ao código-fonte, à esteira de desenvolvimento (*pipeline*), às dependências, aos artefatos, e à implantação (*deploy*).

Quanto ao código, são apresentados controles relacionados às mudanças, ao gerenciamento de repositórios, ao controle de acesso das contribuições, ao controle de fornecedores, aos riscos. E em relação à esteira de desenvolvimento são elencados alguns controles sobre o ambiente de compilação, aos agentes de compilação, às etapas de compilação, à integridade do *pipeline*. Por outro lado em relação às dependências são abordados controles sobre pacotes de terceiros e validação de pacotes. Já quanto aos artefatos são relacionadas atividades sobre a verificação, o acessos dos artefatos, o registro de pacotes e a rastreabilidade da origem. Por fim, sobre a implantação são especificadas ações sobre a configuração e ambiente de *deploy*.

Uma das ferramentas que facilita a implementação do CIS é a Chain-bench que permite auditar a *software supply chain* de maneira a verificar a aderência aos controles de segurança propostos pelo guia [58].

2.5.8 Recomendações da *Cloud Native Computing Foundation* (CNCF)

A comunidade da *Cloud Native Computing Foundation* (CNCF) publicou um documento com um conjunto de recomendações, ferramentas, e considerações de projeto que reduzim a probabilidade e o impacto de um ataque baseado na *supply chain* [59]. Provê um visão holística sobre o assunto, sendo um guia de ponta a ponta para os times de desenvolvimento construírem uma *supply chain* resiliente e verificável.

A plataforma Sigstore desenvolvida pela Linux *Foundation* permite que os desenvolvedores assinem os artefatos de maneira segura [60]. Esses artefatos podem ser binários, imagens de containers, ou até mesmo o SBOM. A plataforma também armazena a assinatura desses artefatos em um registro público resistente a alterações. Também cabe ressaltar que a plataforma não cobra pelo serviço e que o seu código é aberto.

2.6 IDENTIFICAÇÃO DA OPORTUNIDADE DE PESQUISA

Na fase de identificação da oportunidade de pesquisa foi feita uma análise dos trabalhos correlatos detalhados nas Seções 2.5.3 (ENISA), 2.5.4 (SLSA), 2.5.6 (OWASP), 2.5.7 (CIS) e 2.5.8 (CNCF) para verificar se esses estudos implementam as famílias de controles detalhadas em 2.6.1. Com o intuito de facilitar a leitura, é apresentada uma descrição da família de controles antes da apuração de cada trabalho correlato.

2.6.1 Famílias de controles para gerenciamento de riscos da *cyber supply chain*

A integração proposta nesse estudo é baseado nas vinte famílias de controles elencados na publicação especial do NIST acerca do gerenciamento de riscos na *cyber supply chain* [32]. Nas seções a seguir é realizado um breve comentário sobre cada uma dessas famílias de controles.

2.6.1.1 Controle de acesso

O NIST define o requisito de segurança "Controle de acesso" como sendo a restrição imposta pela organização para o acesso às informações dos sistemas apenas por usuários autorizados. Essa definição esta documentada no *Federal Information Processing Standard* (FIPS) 200[61].

O documento [32] cita a necessidade da existência de políticas e procedimentos de controle de acesso. Bem como a obrigação da existência de controles para o gerenciamento de contas e a garantia que as restrições de acesso estão sendo obedecidas.

Outros princípios de segurança também são mencionados como a separação de deveres já discutida na

seção 2.4.1. E o princípio do menor privilégio que preconiza que o usuário deve possuir o menor nível de acesso necessário para a execução de sua atividade.

Outro ponto importante observado é que frequentemente os serviços da *cyber supply chain* realizam acessos remotos, portanto é interessante que sejam implementados controles que implementem técnicas de múltiplo fator de autenticação, restrição do acesso remoto para horários de expediente e apenas para localidades geográficas apropriadas. E também são detalhadas observações sobre o controle de acesso em redes sem fio, e a utilização de dispositivos móveis devido a cultura BYOD conforme já discutido em 2.4.

No relatório da ENISA consta uma recomendação para que os ativos da organização e as informações compartilhadas com os fornecedores tenham procedimentos de controle de acesso bem definidos [6]. Na documentação da SLSA é apresentado o requisito que todos os acessos físicos e remotos devem ser registrados e aprovados por múltiplas partes [49]. No OWASP é elencado o risco de gerenciamento de acesso e identidade inadequado [55]. No guia do CIS existe um conjunto de controles que trata sobre os acessos aos artefatos, inclusive prevendo a impossibilidade de acessar artefatos de maneira anônima [57]. No guia de boas práticas da CNCF existe a previsão que os agentes do *pipeline* de entrega de código e os desenvolvedores humanos tenham os seus acessos calibrados para os seus papéis dentro da organização de maneira a executar apenas atividades permitidas [59].

2.6.1.2 Gerenciamento de configuração

O FIPS 200 afirma que uma organização deve estabelecer e manter uma linha de base de configuração e um inventário dos sistemas de informação [61]. Esse inventário deve conter informações não apenas dos *softwares*, mas também dos *hardwares*. Além disso, é necessário que o inventário seja atualizado durante todo o ciclo de vida do ativo.

Por outro lado, a publicação especial do NIST [32] elenca a necessidade de implementar um controle de gerenciamento de mudanças com o intuito de determinar, implementar, monitorar e auditar mudanças nas configurações dos ativos durante todo o ciclo de vida de desenvolvimento. Também cita a utilização de controles que verificam a assinatura dos componentes para garantir sua autenticidade e integridade, abordagem similar a exposta na seção 2.5.4.

Apesar do relatório da ENISA citar diversas vezes a técnica de ataque que explora vulnerabilidades na configuração dos componentes fornecidos por terceiros, não é feita nenhuma menção para essa família de controles na sua seção de recomendações [6]. Já a documentação da SLSA destaca a utilização da estratégia de *build* como código responsável por compilar os artefatos de acordo com o sistema de versionamento de códigos [49]. No OWASP é citado um risco sobre configuração insegura dos sistemas [55]. No guia do CIS são citados controles de configuração em diferentes partes, como, por exemplo, nas mudanças de código, no ambiente de *build* e na configuração de implantação [57]. No guia de boas práticas da CNCF também é citado o gerenciamento de configuração dos ambientes controlados e na infraestrutura de *build*, inclusive afirmando que o ambiente de compilação deve ter o mesmo nível de segurança do ambiente de operação [59].

2.6.1.3 Manutenção

As organizações devem executar manutenções planejadas periodicamente em seus sistemas informacionais. Essas manutenções devem ser conduzidas por pessoal treinado com ferramentas, técnicas e mecanismos adequados [61].

Adicionalmente, o documento [32] preconiza políticas e procedimentos para que as manutenções sejam conduzidas de maneira segura diminuindo os riscos do comprometimento da *cyber supply chain*. Com esse intuito devem ser escolhidas ferramentas capazes de inspecionar *softwares* e *hardwares*. Além de checar se os controles adequados são adotados tanto pelos membros da organização quanto pelos fornecedores.

No relatório da ENISA existe uma breve menção a um processo de manutenção implementado pelos fornecedores para garantir que sejam observadas as boas práticas de desenvolvimento seguro de produtos e serviços [6]. Na documentação da SLSA e no OWASP não existe previsão pra essa família de controles [49, 55]. No guia do CIS e no guia de boas práticas da CNCF constam alusões ao processo de manutenção de sistemas, mas não existe um controle explícito sobre essa família de controles [57, 59].

2.6.1.4 Proteção dos sistemas e comunicações

Essa família de controles é abordada pelo FIPS 200 [61] como a obrigação das organizações em monitorar, controlar e proteger as comunicações dos sistemas de informação. Essa proteção deve abarcar o projeto de arquitetura, o desenvolvimento de técnicas e princípios de engenharia para promover a segurança efetiva dos sistemas utilizados dentro da organização. Complementarmente, a norma [32] elenca uma diversidade de controles dessa família para proteger à *cyber supply chain*. Pode-se citar a proteção contra ataques de negação de serviço, a salvaguarda da confidencialidade e integridade das transmissões, além da preservação da informação em repouso. Em nenhum dos trabalhos correlatos existe previsão pra essa família de controles [6, 49, 55, 57, 59].

2.6.1.5 Autenticação

O documento do NIST [61] preconiza que a organização deve ser capaz de identificar os usuários dos sistemas de informação. Também deve autenticar processos automatizados que agem como se fossem usuários. Além de autenticar os dispositivos utilizados pelos usuários. Essa verificação dos dispositivos é interessante em um ambiente corporativo por conta do paradigma BYOD e está alinhada com as definições conceituais de Zero Trust apresentadas na Seção 2.4.

No relatório da ENISA existe uma nota de rodapé que cita o uso de múltiplos fatores de autenticação baseada em riscos e um acesso controlado na organização [6]. Na documentação da SLSA também estão presentes requisitos de segurança de autenticação forte utilizando múltiplos fatores de autenticação e a capacidade de verificar a autenticidade dos artefatos utilizados durante o ciclo de desenvolvimento [49]. No OWASP está elencado o risco de validação inapropriada da integridade dos artefatos cujo controle é justamente a garantia da autenticidade [55]. No guia do CIS também é previsto a utilização de autenticação forte em diversos controles, como, por exemplo, a aprovação da submissão de novo código e da revisão de código [57]. No guia de boas práticas da CNCF existe uma previsão sobre todas as entidades que operam

o ambiente da *cyber supply chain* para que sejam ser capazes de se autenticar de maneira segura trocando as chaves com frequência [59].

2.6.1.6 Segurança de pessoal

Essa família de controles sobre segurança de pessoal é definida pelo FIPS 200 [61]. Este documento enaltece que as organizações precisam garantir aos indivíduos que ocupam posições de responsabilidade devem ser confiáveis e devem cumprir com os critérios de segurança estabelecidos para aquela posição. Essas posições também podem ser de prestação de serviços providos por fornecedores.

Um dos controles elencados pelo documento do NIST [32] é a triagem de pessoal. Esse controle consiste em políticas e procedimentos para mitigar riscos de ameaças internas à organização por meio da seleção da equipe responsável pela condução de atividades críticas nos sistemas. Nesse controle cabe destacar a importância da realização dessa triagem também nas equipes dos fornecedores.

No relatório da ENISA existe a previsão da realização da triagem de pessoal nas recomendações de gerenciamento das relações com os fornecedores [6]. Na documentação da SLSA, no OWASP, no guia do CIS e no guia de boas práticas da CNCF não são citados controles sobre segurança de pessoal [49, 55, 57, 59].

2.6.1.7 Processamento de informações pessoais

Acerca dessa família de controles, no Brasil temos vigente a Lei Geral de Proteção de Dados Pessoais (LGPD), que define o tratamento dos dados pessoais com o intuito de proteger os direitos de privacidade e de liberdade [62]. Já no âmbito internacional temos uma variedade de normativos sobre o tema. Para exemplificar, pode-se destacar a *General Data Protection Regulation* (GDPR) da União Europeia [63] e o *California Consumer Privacy Act* (CCPA) do governo do estado da Califórnia, Estados Unidos [64].

Especificamente para gerenciar os riscos da *cyber supply chain*, o NIST preconiza que a organização deve trabalhar junto com seus fornecedores para que as políticas de privacidade e processamento de informações pessoais sejam respeitadas conforme publicação [32]. Esse controle pode ser feito por meio do estabelecimento de políticas e procedimentos que garantam a conformidade com os normativos aplicáveis por toda a *cyber supply chain*.

No relatório da ENISA é afirmado que uma parte dos ataques a *cyber supply chain* visa obter informações pessoais, mas não apresenta um controle dessa família em suas recomendações [6]. Na documentação da SLSA, no OWASP, no guia do CIS não constam controles sobre processamento de informações pessoais [49, 55, 57]. E por fim, no guia de boas práticas da CNCF apenas é citado o processamento de informações pessoais na definição dos riscos dos ambientes, mas não é estipulado um controle [59].

2.6.1.8 Gerenciamento de riscos da *cyber supply chain*

A publicação especial 800-53 do NIST [65] estabelece essa família de controles para o gerenciamento de riscos da *cyber supply chain*. Já o documento 800-161 do NIST [32] detalha as políticas e procedimento

dessa família de controles. Pode-se destacar, a criação de um plano de gerenciamento de riscos, assim como a definição de processos e controles da *cyber supply chain*.

Apenas o guia de boas práticas da CNCF apresenta uma recomendação de controle dessa família [59]. Os demais trabalhos correlatos não possuem controles dessa natureza [6, 49, 55, 57].

2.6.1.9 Avaliação, autorização e monitoramento

Segundo a FIPS 200 [61], a organização deve avaliar frequentemente os controles de segurança para determinar se sua implementação está sendo efetiva. Nessa linha, a organização deve desenvolver e implementar planos de ação para corrigir vulnerabilidades identificadas nos sistemas da informação. E por fim, monitorar os controles de segurança para garantir sua efetividade.

A publicação especial [32] alinhada com a definição feita por [61] cita alguns controles dessa família. Como, por exemplo, a condução de avaliações periódicas dos controles, além da condução de planos de ação e o estabelecimento de marcos para acompanhar melhorias de segurança na *cyber supply chain*. Em nenhum dos trabalhos correlatos existe previsão pra essa família de controles [6, 49, 55, 57, 59].

2.6.1.10 Plano de contingência

A organização deve implementar um plano de resposta a emergências, um plano de operação de *backup* e um plano de recuperação de desastres. Esses planos precisam garantir a disponibilidade dos ativos críticos de tecnologia da informação e a continuidade das operações em situações de emergência [61]. E caso possível a organização deve possuir fornecedores alternativos para soluções críticas [32]

No relatório da ENISA existe uma previsão de obrigar os fornecedores a atenderem os requisitos de continuidade de negócio impostos pelo cliente[6]. Na documentação da SLSA, no OWASP, no guia do CIS e no guia de boas práticas da CNCF não são citados controles dessa natureza [49, 55, 57, 59].

2.6.1.11 Proteção física e de ambiente

A organização deve limitar o acesso físico aos equipamentos para apenas equipes autorizadas [61]. Esse controle geralmente é implementado por portas com fechaduras que utilizam múltiplos fatores de autenticação em *data centers*. Outros controles dessa família são mais relacionados ao ambiente como a proteção contra incêndio e desastres naturais.

Um exemplo mais específico de controle dessa família para a *cyber supply chain* é a proteção contra adulterações. A organização deve exigir e avaliar se o fornecedor implementou mecanismos de proteção contra adulterações em produtos críticos [32].

Na documentação da SLSA existe a previsão que acessos físicos devem feitos por meio de múltiplos fatores de autenticação [49]. Os demais trabalhos correlatos não possuem controles dessa categoria [6, 55, 57, 59].

2.6.1.12 Proteção de mídias

Segundo o guia do NIST [61], as organizações devem proteger as informações armazenadas em mídias limitando o acesso para apenas usuários autorizados. Além disso, os responsáveis pela gestão das mídias devem tomar as devidas providências para destruir as informações quando for descartar ou reutilizar as mídias.

Já a publicação especial [32], enaltece a importância das mídias durante toda a *cyber supply chain*. Esse documento também elenca políticas e procedimentos para a proteção das mídias, como, por exemplo, os controles relacionados ao armazenamento, transporte e higienização das mídias.

Nos trabalhos correlatos não há citação sobre controles de segurança relacionados à proteção das mídias [6, 49, 55, 57, 59].

2.6.1.13 Gerenciamento de programa

A publicação especial 800-53 do NIST sobre controles de segurança e privacidade para sistemas de informação e organizações conceitua o termo "gerenciamento de programa" que é a coordenação de um conjunto de projetos para obter um resultado que não seria possível caso fosse gerenciado por um único projeto[65]. Esse documento define que controles de gerenciamento de programa devem ser implementados em nível estratégico. Esse tipo de controle se aplica à organização como um todo.

Por outro lado, o documento [32] afirma que gerenciamento de programa deve se aplicado a todo o contexto de gerenciamento de riscos da *cyber supply chain*. Nesse guia [32] é estabelecido o papel do líder do programa de segurança da informação responsável por coordenar o programa de implementação de controles. Além disso, nessa publicação [32] são elencados uma série de controles que estruturam esse programa. Pode-se destacar o estabelecimento de um plano de ação com marcos, um conjunto de indicadores de desempenho, e a definição da missão e dos processos de negócio da organização.

Nos trabalhos correlatos não há menção sobre controles de segurança relacionados ao gerenciamento de programa [6, 49, 55, 57, 59].

2.6.1.14 Conscientização e treinamento

O NIST enaltece a importância da organização treinar adequadamente as equipes para que possam realizar suas atividades com o nível de segurança apropriado [61]. Além disso, esses treinamentos devem ser personalizados para que sejam ajustados ao papel exercido pelos integrantes da equipe.

Já a publicação especial [32] elenca uma série de treinamentos mais específicos para a proteção da *cyber supply chain*. Pode-se destacar temas como ameaças internas, engenharia social e *Advanced Persistent Threats* (APTs).

Nos trabalhos correlatos não há menção sobre controles de segurança relacionados a essa família de controles sobre conscientização e treinamento [6, 49, 55, 57, 59].

2.6.1.15 Auditoria e responsabilização

Segundo o NIST, as organizações devem criar, proteger e reter informações sobre registros de auditoria para possibilitar o monitoramento, análise, investigação e reporte de atividades ilícitas, não autorizadas, ou inapropriadas [61]. Por outro lado, a publicação especial [32] destaca a relevância de controles capazes de observar as ocorrências de eventos na *cyber supply chain* dos sistemas da organização. Além da possibilidade de coletar registros dos eventos ocorridos durante todo o ciclo de desenvolvimento. Esses registros devem ser geridos da maneira adequada para que garantam as propriedades de segurança como autenticidade, integridade e não-repúdio.

No relatório da ENISA existem algumas recomendações sobre auditoria, uma delas afirma que os fornecedores devem conduzir auditorias periodicamente para garantir que as boas práticas de segurança elencadas no relatório da ENISA estão sendo implementadas [6]. Na documentação da SLSA não há previsão pra essa família de controles sobre auditoria e responsabilização [49]. No OWASP, um dos riscos mencionados é "Visibilidade e *logs* insuficientes" que reforça a importância da identificação e coleta das fontes de registros de eventos [55]. No guia do CIS existem controles relacionados a auditoria de mudanças de código e de pacotes [57]. No guia de boas práticas da CNCF é sugerido a utilização de *Infrastructure as code* (IaC) para possibilitar a auditoria do processo de construção dos ambientes dos sistemas [59].

2.6.1.16 Integridade das informações

As organizações devem identificar, reportar e corrigir falhas nas informações e nos sistemas de informação em um tempo adequado [61]. Os sistemas de informação e os componentes utilizados ao longo da *cyber supply chain* devem ter a integridade de suas informações garantidas para que se possam gerenciar os riscos da cadeia de fornecimento [32].

Apesar do relatório da ENISA, da documentação da SLSA, do guia do CIS e do guia de boas práticas da CNCF citarem controles para garantir a integridade dos artefatos, não é feita uma menção sobre integridade das informações [6, 49, 57, 59]. No OWASP é detalhado o risco de uma validação inapropriada da integridade dos artefatos, porém também não é mencionado um controle específico para a integridade das informações [55].

2.6.1.17 Planejamento

A organização deve implementar planos de melhorias dos aspectos de segurança cibernética dos seus sistemas de informação [61]. Esses planos devem ser documentados e atualizados com frequência. Além disso, devem descrever detalhadamente o estado atual e o futuro dos controles de segurança. Já o [32] preconiza que a família de controles de planejamento deve fazer parte do gerenciamento de riscos da *cyber supply chain*.

Nos trabalhos correlatos não há alusão sobre controles de segurança relacionados ao planejamento de melhorias na segurança da *cyber supply chain* [6, 49, 55, 57, 59].

2.6.1.18 Aquisição de sistemas e serviços

As organizações devem alocar recursos suficientes para proteger adequadamente os sistemas de informação [61]. Essa alocação de recursos pode ser feita por meio da aquisição de *software* de terceiros que implementam medidas de segurança adequadas durante o seu ciclo de desenvolvimento. A publicação [32] cita uma série de controles dessa família. Alguns deles relacionados ao estabelecimento de políticas e procedimentos para aquisição de sistemas e serviços de terceiros. Além de outros controles associados ao ciclo de desenvolvimento de sistemas e ao processo de aquisição.

Nos trabalhos correlatos não há menção sobre controles de segurança relacionados a essa família de controles sobre aquisição de sistemas e serviços [6, 49, 55, 57, 59].

2.6.1.19 Resposta a incidentes

O FIPS 200 [61] especifica que as organizações devem ser capazes de tratar incidentes em sistemas da informação. Isso inclui o adequado planejamento, detecção, análise, recuperação e atividades de resposta aos usuários. A norma [32] prevê a escrita de políticas, treinamentos, monitoramento e reporte sobre resposta a incidentes na *cyber supply chain*.

No relatório da ENISA existe a menção da utilização de uma taxonomia da União Europeia para facilitar a coordenação de atividades relacionadas à resposta a incidentes, porém não é detalhado um controle específico [6]. Na documentação da SLSA também não existe um controle sobre resposta a incidentes [49]. No OWASP é citada a importância da existência de um registro centralizado dos eventos dos sistemas como sendo primordial para um cenário de resposta a incidentes, porém também não é esmiuçado um controle dessa família [55]. No guia do CIS também não é elencado um controle dessa natureza [57]. No guia de boas práticas da CNCF exige que os fornecedores possuam equipes de resposta a incidentes com nível de acordo estabelecido, porém não discrimina um controle dessa natureza [59].

2.6.1.20 Avaliação de riscos

Segundo a publicação do NIST [61], as organizações devem avaliar periodicamente os riscos operacionais resultantes da utilização dos sistemas e do processamento, armazenamento e transmissão de suas informações. Já a publicação especial 800-161 do NIST preconiza que existam políticas e procedimentos para o gerenciamentos de riscos da *cyber supply chain* [32]. Também prevê que as vulnerabilidades de todos os produtos inclusive dos *softwares* fornecidos por terceiros sejam constantemente monitorados.

No relatório da ENISA consta uma sugestão às autoridades competentes dos países da União Europeia para que realizem avaliações de riscos da *cyber supply chain* de infraestruturas críticas afim de derivar medidas de proteção em nível nacional, porém não detalha controles dessa natureza [6]. Na documentação da SLSA, no OWASP, no guia do CIS, no guia de boas práticas da CNCF não há previsão de controles de avaliação de riscos na *cyber supply chain* [49, 55, 57, 59].

2.6.2 Comparação de implementação das famílias de controles

Por meio do estudo dos trabalhos correlatos foi possível identificar um oportunidade de pesquisa. Verificou-se que os trabalhos existentes não cobrem todas famílias de controles identificadas pelo NIST em [32] conforme exposto na Seção 2.6.1 e resumido pela tabela comparativa 2.5. Desta forma, no capítulo a seguir é proposto um conjunto de controles baseados na abordagem *Zero Trust* mitigando os riscos da publicação especial do NIST [32].

Tabela 2.5: Família de controles implementados pelos trabalhos correlatos

Controles\Trabalhos correlatos	ENISA	SLSA	OWASP	CIS	CNCF
Controle de acesso	✓	✓	✓	✓	✓
Gerenciamento de configuração		✓	✓	✓	✓
Manutenção	✓				
Proteção dos sistemas e comunicações					
Autenticação	✓	✓	✓	✓	✓
Segurança de pessoal	✓				
Processamento de informações pessoais					
Gerenciamento de riscos da cyber supply chain					✓
Avaliação, autorização e monitoramento					
Plano de contingência	✓				
Proteção física e de ambiente		✓			
Proteção de mídias					
Gerenciamento de programa					
Conscientização e treinamento					
Auditoria e responsabilização	✓		✓	✓	✓
Integridade das informações					
Planejamento					
Aquisição de sistemas e serviços					
Resposta a incidentes					
Avaliação de riscos					

3 PROPOSTA DE INTEGRAÇÃO DE CONTROLES DE SEGURANÇA BASEADOS NOS PRINCÍPIOS *ZERO TRUST* EM UMA *CYBER SUPPLY CHAIN*

A proposta deste trabalho é composta de vinte controles classificados em seis domínios. Esses controles são baseados em sete princípios *Zero Trust*, sendo que cada controle possui três estágios de implementação (básico, intermediário e avançado). Resumidamente, *Zero Trust* é um abordagem que norteia o desenho de arquiteturas de redes e sistemas considerando ameaças internas e o monitoramento contínuo. Essa abordagem ganhou notoriedade no mercado de tecnologia por endereçar alguns problemas presentes em infraestruturas críticas. E pode ser representada por meio de conceitos elencados na Seção 2.4 e também por um conjunto de princípios enumerados na Seção 2.4.1. A figura 3.1 ilustra a estrutura dessa proposta.

Figura 3.1: Estrutura da proposta de integração de controles *Zero Trust* em uma *cyber supply chain*

A proposta de integração é divida em etapas. O primeiro passo é a identificação dos componentes críticos da *cyber supply chain*. Logo em seguida, é verificada a aderência aos controles baseados nos princípios *Zero Trust*, de maneira a permitir uma análise de *gap* dos controles que ainda precisam ser implementados. E por fim, o desenho de um *roadmap* de implementação das melhorias de segurança identificadas por meio das visualizações sugeridas. As etapas citadas acima estão ilustradas na figura 3.2.

3.1 MENSURAÇÃO DA ADERÊNCIA AOS CONTROLES BASEADOS NOS PRINCÍPIOS DE *ZERO TRUST*

O primeiro passo da análise consiste em realizar uma decomposição da solução nos componentes da *cyber supply chain*. Um insumo importante para essa etapa é o artefato denominado *Software Bill of Materials* (SBOM) [12], explicado na seção 2.3.

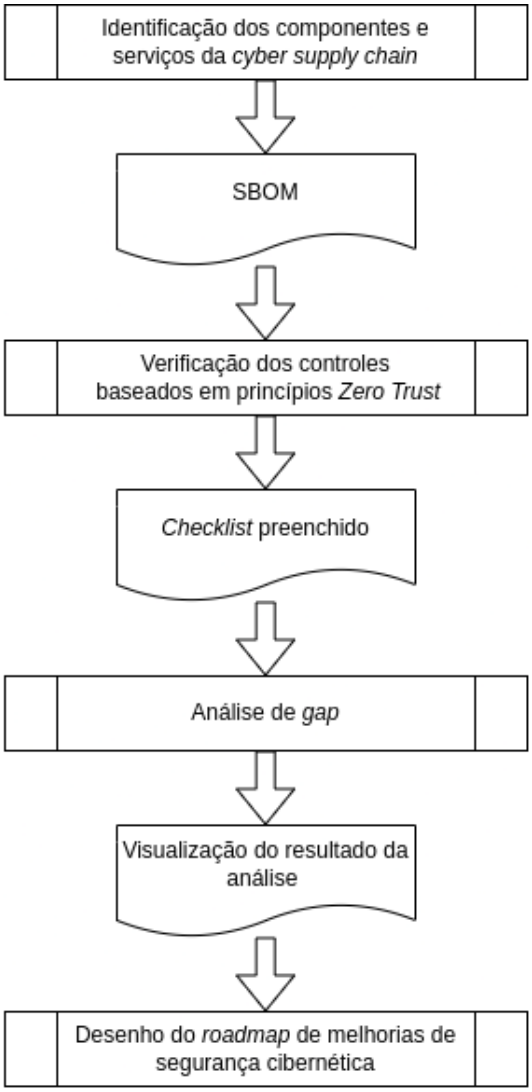

Figura 3.2: Etapas da proposta de integração de controles baseados nos princípios *Zero Trust* na proteção de uma *cyber supply chain*

Após a identificação dos componentes da *cyber supply chain* da solução, deve-se realizar uma análise individual de cada componente de maneira a verificar a aderência aos controles baseados nos princípios de *Zero Trust*. Nesse estudo são explorados os princípios enunciados pela publicação do NIST 800-207 [23]. É sugerida uma adaptação para que utilize a palavra "organização" em vez de "empresa", por se tratar de um termo mais abrangente que engloba empresas privadas, órgãos de governo e organizações sem fins lucrativos. Os princípios são apresentados logo a seguir:

- P1. Todas as fontes de dados e serviços computacionais são considerados recursos;
- P2. Toda comunicação é protegida independente de sua localização;
- P3. O acesso aos recursos individuais da organização é concedido para cada sessão;
- P4. O acesso aos recursos é determinado por uma política atualizada dinamicamente;
- P5. A organização monitora a integridade e segurança de todos os ativos;
- P6. Toda autenticação e autorização de recursos é dinâmica e estritamente aplicada antes que o acesso seja concedido;
- P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança.

Com a finalidade de organizar os controles, este trabalho sugere seis domínios adaptados do *Zero Trust Guidance Center* da *Microsoft* [66] e do *Zero Trust Maturity Model* [33] da CISA, elencados abaixo:

- Infraestrutura e redes (D1): utilização de telemetria para detectar ataques e anomalias, e possibilitar a tomada de ações proativas. Segmentação da rede, implantação de proteções em tempo real, cifração de dados de ponta a ponta, monitoração e análise.
- Identidade (D2): verificação de identidade de pessoas, serviços ou dispositivos;
- Dispositivo (D3): monitoração e garantia de conformidade dos dispositivos para se ter um acesso seguro;
- Governança e dados (D4): conjunto de políticas e procedimentos que estabelecem como a organização detecta, previne e responde a incidentes cibernéticos. Além da classificação e proteção dos dados;
- Aplicação (D5): uso de configurações seguras e monitoração em tempo real;
- DevSecOps e ciência de dados (D6): integração das atividades inerentes ao desenvolvimento, segurança e operação das aplicações. Além de permitir a visualização e análise dos dados;

Os domínios "Governança e dados" e "DevSecOps e ciência de dados" permeiam todos os controles. Também cabe explicar que foi escolhido o termo "DevSecOps e ciência de dados" em vez da nomenclatura

original do guia da *Microsoft* "Visibilidade, Automação e Orquestração", pois aquele termo sintetiza melhor um conjunto de atividades mais focado em segurança cibernética e também por ser mais reconhecido na literatura [67]. Além disso, "ciência de dados" abrange mais atividades do que apenas a visualização dos dados.

3.2 CONTROLES PROPOSTOS EM UM FORMATO DE *CHECKLIST*

A partir dos princípios e domínios apresentados, essa pesquisa apresenta uma proposta de *checklist* baseado nas famílias de controles apresentados no guia do NIST [32]. Cada controle é dividido em três estágios de adoção "básico" (S.1), "intermediário" (S.2) e "avançado" (S.3). Esses estágios refletem o grau de aderência aos controles propostos baseados nos princípios *Zero Trust*. Levando em consideração a estrutura explicada, a proposta dos controles é apresentada nas seções a seguir que detalham cada domínio da integração.

3.2.1 Infraestrutura e redes (D1)

O primeiro domínio trata da proteção da infraestrutura e redes. Com essa finalidade são adotados alguns princípios *Zero Trust*, como, por exemplo, "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança". Nesse domínio são implementados mecanismos de controle de acesso, gerenciamento de configuração, manutenção e proteção dos sistemas e comunicações. Nas próximas seções são apresentados os controles citando alguns princípios *Zero trust* que devem ser respeitados durante suas implementações. E por último, a tabela 3.1 representa os controles do domínio "Infraestrutura e redes (D1)".

3.2.1.1 Controle de acesso (C1)

O controle de acesso é fundamental para a adequada proteção da *cyber supply chain* conforme já exposto em 2.6.1.1. A primeira etapa a ser implementada nesse controle é o estabelecimento de uma política de acesso que considera pelo menos os princípios *Zero Trust* "P3. O acesso aos recursos individuais da organização é concedido para cada sessão" e "P4. O acesso aos recursos é determinado por uma política atualizada dinamicamente". Além disso, essa política deve considerar as relações com os fornecedores e o controle do acesso dos componentes de terceiros.

Em um segundo momento, deve-se implementar ações que garantam a observância da política. Destaca-se as ações relacionadas ao controle de acesso de cada sessão, desta forma evita-se que uma sessão autenticada no passado possa realizar novas atividades sem ser autorizado novamente, uma confiança "herdada". Importante destacar, ainda, que as revisões periódicas do controle de acesso devem ser feitas de acordo com o princípio *Zero Trust* "P4. O acesso aos recursos é determinado por uma política atualizada dinamicamente". E por fim, outras boas práticas de segregação de deveres, mínimo acesso necessário e microsegmentação também devem ser seguidos conforme discutido em 2.4.1.

E numa etapa mais avançada, é interessante que a telemetria dos acessos seja capaz de fornecer subsídios para a tomada de decisões em tempo real e que ações dos usuários sejam completamente rastreáveis. Assim, o ambiente de infraestrutura e redes estaria mais protegido e seria mais fácil de detectar fragilidades nos acessos dos componentes da *cyber supply chain*. Apenas para resumir seguem os níveis desse controle em formato de *checklist*.

- Básico (S.1): Existe uma política de acesso que considera aspectos da *cyber supply chain* ?
- Intermediário (S.2): O controle de acesso é executado em cada sessão ?
  As permissões de acesso são revisadas periodicamente ?
  É concedido o mínimo acesso necessário para que os usuários possam executar suas atividades ?
  As permissões de acesso são segregadas ?
  É realizada uma microsegmentação da rede ?
- Avançado (S.3): O controle de acesso é baseado em uma política atualizada dinamicamente que permite a tomada de decisões em tempo real ?
  É possível rastrear todas as ações dos usuários ?

3.2.1.2 Gerenciamento de configuração (C2)

O gerenciamento de configuração permite um controle mais seguro dos componentes da *cyber supply chain*. Cabe destacar que segundo o princípio *Zero Trust* "P5. A organização monitora a integridade e segurança de todos os ativos". Com isso em vista, é necessário em um primeiro momento o estabelecimento de uma política de gerenciamento de configuração assim como procedimentos relacionados aos ativos da *cyber supply chain*.

Em uma fase intermediária, deve-se estabelecer uma linha de base de configuração dos componentes da *cyber supply chain* fornecendo informações cruciais para sua proteção, como, por exemplo, versões, *hashes* e assinaturas que permitam a implementação de outros controles. E numa etapa mais avançada, o gerenciamento de configuração deve ser incorporado numa esteira de desenvolvimento automatizada baseada nos conceitos de DevSecOps. Assim, nessa última etapa seria possível lidar com as mudanças dos componentes de uma maneira dinâmica permitindo decisões mais céleres. Apenas para sintetizar seguem os níveis expostos desse controle em formato de *checklist*.

- Básico (S.1): Existe uma política definida sobre como realizar o gerenciamento de configuração da *cyber supply chain* ?
  Existem procedimentos sobre como adicionar ou remover componentes do ambiente organizacional ?
- Intermediário (S.2): Existe uma linha de base da configuração da *cyber supply chain* ?
  Existe um controle de mudanças de configuração estabelecido ?
- Avançado (S.3): O controle de mudanças de configuração é automatizado ?
  É possível analisar dinamicamente impactos de maneira a permitir a tomada de decisões em tempo

real ?

3.2.1.3 Manutenção (C3)

A *cyber supply chain* sofre manutenções constantemente, portanto devem existir controles de segurança cibernética nessa temática conforme discutido em 2.6.1.3. Esses controles devem seguir os princípios *Zero Trust* "P1. Todas as fontes de dados e serviços computacionais são considerados recursos" e "P5. A organização monitora a integridade e segurança de todos os ativos". No nível básico, devem ser implementadas políticas e procedimentos para orientar as manutenções segundo os princípios citados. Em um segundo momento, devem ser compartilhadas informações sobre as manutenções da *cyber supply chain* para fornecer uma proteção mais adequada. E em um nível mais avançado, as atividades relacionadas às manutenções devem ser automatizadas para diminuir o risco da intervenção humana e facilitar o rastreio das mudanças, bem como melhorar o monitoramento. A seguir esses níveis são apresentados em formato de *checklist*.

- Básico (S.1): Existem políticas e procedimentos para a manutenção da *cyber supply chain ?*
- Intermediário (S.2): As informações sobre as manutenções são compartilhadas levando em consideração aspectos de uma arquitetura *Zero Trust* ?
- Avançado (S.3): As atividades de manutenção da *cyber supply chain* são automatizadas ?
  As manutenções são continuamente monitoradas ?

3.2.1.4 Proteção dos sistemas e comunicações (C4)

A proteção dos sistemas e comunicações deve seguir os princípios *Zero Trust* "P2. Toda comunicação é protegida independente de sua localização" e "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança". Assim no nível básico, deve ser estabelecida uma política de proteção das comunicações dos elementos da *cyber supply chain*. Num segundo momento de acordo com os princípios *Zero trust*, as ameaças internas são consideradas e é implementada uma abordagem de segurança em camadas, conhecida também pela analogia da cebola, onde não é possível atingir o núcleo crítico do sistema sem antes ter passado por diversas camadas de proteção. E por fim, no nível mais avançado são utilizadas técnicas de ciência de dados para monitorar, analisar e adaptar constantemente as proteções. Seguem os níveis em formato de *checklist*, adiante:

- Básico (S.1): Existe uma política de proteção das comunicações utilizadas na *cyber supply chain* ?
- Intermediário (S.2): A organização protege suas fronteiras considerando ameaças internas ?
  As comunicações são protegidas em diversas camadas heterogêneas considerando possíveis falhas em alguns mecanismos ?
- Avançado (S.3): Os mecanismos de proteção das comunicação são monitorados e adaptados continuamente?

Tabela 3.1: Os controles propostos do domínio "Infraestrutura e redes (D1)" organizados por domínios e estágios.

Domínio e controles\Estágios		Básico (S.1)	Intermediário (S.2)	Avançado (S.3)
Infraestrutura e redes (D1)	**Controle de acesso (C1)**	Existe uma política de acesso que considera aspectos da *cyber supply chain* ?	O controle de acesso é executado em cada sessão ? As permissões de acesso são revisadas periodicamente ? É concedido o mínimo acesso necessário para que os usuários possam executar suas atividades ? As permissões de acesso são segregadas ? É realizada uma microsegmentação da rede ?	O controle de acesso é baseado em uma política atualizada dinamicamente que permite a tomada de decisões em tempo real ? É possível rastrear todas as ações dos usuários ?
	Gerenciamento de configuração (C2)	Existe uma política definida sobre como realizar o gerenciamento de configuração da *cyber supply chain* ? Existem procedimentos sobre como adicionar ou remover componentes do ambiente organizacional ?	Existe uma linha de base da configuração da *cyber supply chain* ? Existe um controle de mudanças de configuração estabelecido ?	O controle de mudanças de configuração é automatizado ? É possível analisar dinamicamente impactos de maneira a permitir a tomada de decisões em tempo real ?
	Manutenção (C3)	Existem políticas e procedimentos para a manutenção da *cyber supply chain* ?	As informações sobre as manutenções são compartilhadas levando em consideração aspectos de uma arquitetura *Zero Trust* ?	As atividades de manutenção da *cyber supply chain* são automatizadas ? As manutenções são continuamente monitoradas ?
	Proteção dos sistemas e comunicações (C4)	Existe uma política de proteção das comunicações utilizadas na *cyber supply chain* ?	A organização protege suas fronteiras considerando ameaças internas ? As comunicações são protegidas em diversas camadas heterogêneas considerando possíveis falhas em alguns mecanismos ?	Os mecanismos de proteção das comunicação são monitorados e adaptados continuamente?

3.2.2 Identidade (D2)

O segundo domínio foca em questões de identidade e gerenciamento de riscos com os fornecedores. Para que a *cyber supply chain* seja protegida adequadamente devem ser verificadas as identidades das pessoas, serviços e dispositivos envolvidos. Cabe destacar que devem ser observado o princípio *Zero Trust* "Toda autenticação e autorização de recursos é dinâmica e estritamente aplicada antes que o acesso seja concedido". Esse domínio agrupa os controles relacionados a autenticação, segurança de pessoal, processamento de informações pessoais e gerenciamento de riscos da *cyber supply chain*. E por último, a tabela 3.2 elenca os controles do domínio "Identidade (D2)".

3.2.2.1 Autenticação (C5)

Segundo os princípios *Zero Trust*, a autenticação deve ser realizada antes que o acesso seja concedido e precisa ser dinâmica no aspecto que deve ser contínua para cada sessão estabelecida. Em um primeiro momento, deve-se estabelecer uma política de autenticação para os componentes e serviços da *cyber supply chain*.

Em uma etapa intermediária, deve-se gerir a identidade das pessoas, serviços e dispositivos envolvidos durante todo o ciclo de vida dos componentes da *cyber supply chain*. Além da adoção de um mecanismo de autenticação forte por meio de múltiplos fatores de preferência com o uso de biometria ("o que você é") e *tokens* ("o que você possui"), em detrimento de senhas ("o que você sabe") devido a fragilidade decorrente de vazamentos de informações de senhas.

No terceiro nível, deve-se adotar técnicas de ciência de dados como aprendizado de máquina para a implementação de políticas mais dinâmicas capazes de oferecer uma proteção mais tempestiva. Essas técnicas auxiliam a exploração dos dados de comportamentos prévios e possibilitam determinar qual é o acesso mínimo necessário de acordo com a análise realizada. Na sequência, esses três níveis são apresentados num formato de *checklist*.

- Básico (S.1): Existe uma política de autenticação na *cyber supply chain* ?
- Intermediário (S.2): É realizada a gestão da identidade na *cyber supply chain* ?
  São utilizados múltiplos fatores de autenticação ?
- Avançado (S.3): A autenticação é baseada em uma política atualizada dinamicamente permitindo decisões em tempo real ?

3.2.2.2 Segurança de pessoal (C6)

A *cyber supply chain* é composta de componentes de *software* fornecidos por terceiros e também de serviços entregues por pessoas. Desta forma, é importante implementar controles atentos aos aspectos de segurança inerentes ao elemento humano. Por outro lado, segundo o princípio *Zero Trust* "P1. Todas as fontes de dados e serviços computacionais são considerados recursos" é importante enfatizar que deve-se considerar todos os serviços como recursos que precisam ser protegidos.

Assim em um nível básico de implementação desse controle, deve-se estabelecer uma política de segurança de pessoal com questões inerentes a proteção da *cyber supply chain*. Depois em uma etapa intermediária, deve-se conduzir ações capazes de realizar uma investigação social na equipe contratada para atuar em componentes críticos da *cyber supply chain*. E por último num estágio mais avançado, os mecanismos de verificação de aderência a política adotada são automatizados para que possa ser implementado um ciclo de melhoria contínua. Esses níveis estão expostos a seguir em um formato de *checklist*.

- Básico (S.1): Existe uma política de segurança de pessoal considerando aspectos de segurança da cyber supply chain ?
- Intermediário (S.2): É realizada uma investigação social na contratação de empregados que irão atuar em componentes críticos da *cyber supply chain* ?
  Existe um monitoramento do comportamento de pessoas que atuam na infraestrutura crítica ?
- Avançado (S.3): Os mecanismos de verificação do cumprimento da política de segurança de pessoal são monitorados e aprimorados continuamente ?

3.2.2.3 Processamento de informações pessoais (C7)

Conforme já discutido no referencial teórico na Seção 2.6.1.7, atualmente existem uma série de normativos e leis acerca do manuseio de informações pessoais que preconizam alguns controles de segurança cibernética. Esses controles devem observar o princípio *Zero Trust* "P2. Toda comunicação é protegida independente de sua localização", pois as informações pessoais devem ser protegidas mesmo sendo armazenadas em sistemas internos da organização.

Desta forma, em um estágio básico de implementação desses controles deve-se estabelecer uma política de processamento de informações pessoais considerando todas as fontes de dados e serviços computacionais. Em um segundo momento, é preciso implementar proteções independente da localização dos dados pessoais protegendo de ameaças externas e internas. E no estágio mais avançado, esses mecanismos devem ser automatizados para que se possa responder de maneira rápida a possíveis violações de segurança. Levando em consideração essa discussão, os três níveis são apresentados a seguir em formato de *checklist*.

- Básico (S.1): Existe uma política de processamento de informações pessoais aplicada na *cyber supply chain* ?
- Intermediário (S.2): Os dados pessoais são manipulados de maneira adequada considerando tanto ameaças internas quanto externas à organização ?
- Avançado (S.3): Os mecanismos de proteção de dados pessoais são atualizados constantemente ?

3.2.2.4 Gerenciamento de riscos da *cyber supply chain* (C8)

O gerenciamento de riscos da *cyber supply chain* é catalogado como uma das famílias de controles necessárias para a proteção adequada da cadeia de fornecimento pelo documento do NIST [32] conforme

já discutido em 2.6.1.8. Em um primeiro estágio, a organização deve estabelecer uma política que deve estabelecer obrigações e fornecer orientações sobre o gerenciamento de riscos seguindo pelo menos os princípios *Zero Trust* "P1. Todas as fontes de dados e serviços computacionais são considerados recursos", "P5. A organização monitora a integridade e segurança de todos os ativos" e "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança".

Em um passo intermediário de implementação desse controle, a organização deve construir um inventário de fornecedores e ser capaz de verificar as assinaturas dos mesmos para garantir a autenticidade dos componentes desenvolvidos por terceiros. E por último em um estágio mais avançado, deve-se implementar mecanismos capazes de atualizar constantemente os planos de gerenciamento de riscos com base em elementos coletados automaticamente. Por fim, apresenta-se esses níveis em um formato de *checklist*.

- Básico (S.1): Existe uma política de gerenciamento dos riscos da *cyber supply chain* ?
- Intermediário (S.2): Existe um inventário dos fornecedores e é possível verificar a autenticidade dos componentes da *cyber supply chain* ?
- Avançado (S.3): O plano de gerenciamento dos riscos da *cyber supply chain* é atualizado frequentemente baseado em insumos coletados automaticamente ?

3.2.3 Dispositivo (D3)

O terceiro domínio se preocupa com questões de segurança relacionadas ao monitoramento e garantia de conformidade dos dispositivos. Nesse domínio são agrupados os controles sobre avaliação, autorização, monitoramento, plano de contingência, proteção física e de ambiente, e proteção de mídias. Por último, a tabela 3.3 expõe os controles do domínio "Dispositivo (D3)".

3.2.3.1 Avaliação, autorização e monitoramento (C9)

Conforme já debatido na Seção 2.6.1.9 no capítulo de trabalhos correlacionados, a organização deve constantemente avaliar a eficácia dos controles de segurança implementados. Na temática desse trabalho, essa avaliação também deve ser considerar controles de segurança cibernética da *cyber supply chain* tendo em vista no mínimo os princípios *Zero Trust* "P5. A organização monitora a integridade e segurança de todos os ativos" e "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infra- estrutura de rede e comunicações e as usa para melhorar sua política de segurança".

Em um primeiro momento, a organização deve estabelecer uma política de avaliação dos controles de segurança relacionados à *cyber supply chain* baseada nos princípios já expostos. Depois, em um nível intermediário deve ser implementado um plano de ações com a previsão de marcos de avaliação dos controles. E no último nível, são utilizadas técnicas de ciência de dados para identificação de tendências de riscos à *cyber supply chain* para permitir a tomada de decisões tempestivas. Considerando o debate aqui realizado seguem os níveis do controle em formato de *checklist*.

Tabela 3.2: Os controles propostos do domínio "Identidade (D2)" organizados por domínios e estágios.

Domínio e controles\Estágios		**Básico (S.1)**	**Intermediário (S.2)**	**Avançado (S.3)**
Identidade (D2)	**Autenticação (C5)**	Existe uma política de autenticação na *cyber supply chain* ?	É realizada a gestão da identidade na *cyber supply chain* ? São utilizados múltiplos fatores de autenticação ?	A autenticação é baseada em uma política atualizada dinamicamente permitindo decisões em tempo real ?
	Segurança de pessoal (C6)	Existe uma política de segurança de pessoal considerando aspectos de segurança da *cyber supply chain* ?	É realizada uma investigação social na contratação de empregados que irão atuar em componentes críticos da *cyber supply chain* ? Existe um monitoramento do comportamento de pessoas que atuam na infraestrutura crítica ?	Os mecanismos de verificação do cumprimento da política de segurança de pessoal são monitorados e aprimorados continuamente ?
	Processamento de informações pessoais (C7)	Existe uma política de processamento de informações pessoais aplicada na *cyber supply chain* ?	Os dados pessoais são manipulados de maneira adequada considerando tanto ameaças internas quanto externas à organização ?	Os mecanismos de proteção de dados pessoais são atualizados constantemente ?
	Gerenciamento de riscos da *cyber supply chain* (C8)	Existe uma política de gerenciamento dos riscos da *cyber supply chain* ?	Existe um inventário dos fornecedores e é possível verificar a autenticidade dos componentes da *cyber supply chain* ?	O plano de gerenciamento dos riscos da *cyber supply chain* é atualizado frequentemente baseado em insumos coletados automaticamente ?

- Básico (S.1): A política de segurança da informação da organização incorpora aspectos de avaliação da *cyber supply chain* ?
- Intermediário (S.2): Existe um plano de ações e marcos de avaliação da *cyber supply chain* ?
- Avançado (S.3): É realizado um monitoramento contínuo analisando tendências de forma a possibilitar a tomada de decisão em tempo real ?

3.2.3.2 Plano de contingência (C10)

O plano de contingência é primordial em situações de emergência. E é interessante que os fornecedores sejam obrigados a atender alguns requisitos de continuidade de negócio conforme discutido em 2.6.1.10. Além disso, o plano de contingência deve considerar pelo menos os princípios *Zero Trust* "P1. Todas as fontes de dados e serviços computacionais são considerados recursos" e "P2. Toda comunicação é protegida independente de sua localização".

Levando isso em consideração em um estágio básico de implementação dos controles, a organização deve estabelecer um plano de contingência considerando os componentes e serviços prestados por terceiros. Em um estágio intermediário, deve-se identificar os ativos críticos da *cyber supply chain* que necessitam de um plano de contingência mais refinado. E no nível mais avançado, a organização deve ser capaz de prestar serviços alternativos com a segurança adequada. Por fim, apenas para resumir seguem os níveis desse controle em formato de *checklist*.

- Básico (S.1): Existe um plano de contingência para a *cyber supply chain* ?
- Intermediário (S.2): Os ativos críticos da *cyber supply chain* são identificados ?
- Avançado (S.3): A organização é capaz de prestar serviços alternativos considerando aspectos de uma arquitetura *Zero Trust* ?

3.2.3.3 Proteção física e de ambiente (C11)

A proteção física e de ambiente é necessária para a adequada proteção dos componentes e serviços prestados por terceiros. Esses controles de segurança devem observar pelo menos os princípios *Zero Trust* "P2. Toda comunicação é protegida independente de sua localização", "P3. O acesso aos recursos individuais da organização é concedido para cada sessão" e "P4. O acesso aos recursos é determinado por uma política atualizada dinamicamente". É interessante que seja seguida uma boa prática de construção de barreiras de retardo progressivas para a defesa dos ativos físicos.

Em um primeiro momento, convém destacar a importância de a organização estabelecer uma política de proteção física e de ambiente, considerando que a equipe de fornecedores deve possuir o acesso mínimo necessário ao ambiente físico para a condução de suas atividades. No segundo momento, o acesso físico deve ser segregado por papéis baseados nas atividades realizadas, com a implementação de mecanismos de proteção contra modificações físicas. Um exemplo de proteção dessa natureza são mecanismos *tamper-proof* utilizados em *Hardware security modules* (HSMs) capazes de detectar tentativas de acesso às chaves

criptográficas armazenadas em equipamentos críticos. E em um nível mais avançado esses ativos são monitorados e rastreados continuamente por meio de controles automatizados. Considerando o exposto seguem os níveis em formato de *checklist*.

- Básico (S.1): Existe uma política de proteção física e de ambiente ?
- Intermediário (S.2): O acesso físico é segregado por papéis ?
  Existe uma proteção contra modificações físicas?
- Avançado (S.3): Os ativos são monitorados e rastreados continuamente ?

3.2.3.4 Proteção de mídias (C12)

Diversas mídias são utilizadas durante toda a *cyber supply chain*, desta forma essas mídias devem ser protegidas de maneira adequada conforme discutido em 2.6.1.12. Para isso deve-se adotar no mínimo os princípios *Zero Trust* "P1. Todas as fontes de dados e serviços computacionais são considerados recursos" e "P2. Toda comunicação é protegida independente de sua localização".

No nível básico de implementação do controle, deve-se estabelecer uma política de proteção das mídias utilizadas na *cyber supply chain* com o emprego de criptografia adequada de acordo com o nível de sensibilidade da informação. No nível intermediário, a organização deve implementar procedimentos de sanitização lógica e física das mídias para possibilitar o reúso quando possível ou o descarte correto dos equipamentos em cenários de maior risco. E no nível mais avançado, deve-se existir mecanismos que permitem o monitoramento contínuo das mídias durante todo o seu ciclo de vida permitindo a tomada de decisões céleres. Por último, apresenta-se os níveis em formato de *checklist*.

- Básico (S.1): Existe uma política de proteção de mídias utilizadas na *cyber supply chain* ?
  A organização emprega criptografia na proteção de dados sensíveis nas mídias ?
- Intermediário (S.2): A organização sanitiza as mídias ?
- Avançado (S.3): Existe um monitoramento contínuo das mídias que possibilita a tomada de decisões em tempo real ?

3.2.4 Governança e dados (D4)

O quarto domínio "Governança e dados (D4)" aborda um conjunto de políticas e procedimentos que definem como a organização detecta, previne e responde aos incidentes cibernéticos da *cyber supply chain*. Além disso, apresenta uma preocupação com a classificação e proteção dos dados. Nesse domínio são agrupados os controles gerenciamento de programa, conscientização, treinamento, auditoria, responsabilização, integridade das informações e planejamento. A tabela 3.4 contém os controles desse domínio.

Tabela 3.3: Os controles propostos do domínio "Dispositivo (D3)" organizados por domínios e estágios.

Domínio e controles\Estágios		**Básico (S.1)**	**Intermediário (S.2)**	**Avançado (S.3)**
Dispositivo (D3)	**Avaliação, autorização e monitoramento (C9)**	A política de segurança da informação da organização incorpora aspectos de avaliação da *cyber supply chain* ?	Existe um plano de ações e marcos de avaliação da *cyber supply chain* ?	É realizado um monitoramento contínuo analisando tendências de forma a possibilitar a tomada de decisão em tempo real ?
	Plano de contingência (C10)	Existe um plano de contingência para a *cyber supply chain* ?	Os ativos críticos da *cyber supply chain* são identificados ?	A organização é capaz de prestar serviços alternativos considerando aspectos de uma arquitetura *Zero Trust* ?
	Proteção física e de ambiente (C11)	Existe uma política de proteção física e de ambiente ?	O acesso físico é segregado por papéis ? Existe uma proteção contra modificações físicas?	Os ativos são monitorados e rastreados continuamente ?
	Proteção de mídias (C12)	Existe uma política de proteção de mídias utilizadas na *cyber supply chain* ? A organização emprega criptografia na proteção de dados sensíveis nas mídias ?	A organização sanitiza as mídias ?	Existe um monitoramento contínuo das mídias que possibilita a tomada de decisões em tempo real ?

3.2.4.1 Gerenciamento de programa (C13)

O gerenciamento de programas é a coordenação de um conjunto de projetos com o intuito de promover melhorias de segurança na *cyber supply chain* conforme já discutido na Seção 2.6.1.13 do capítulo de trabalhos correlatos. Em um primeiro nível de implementação desse controle, deve-se estabelecer um programa de atividades para o aperfeiçoamento da segurança dos componentes e serviços da *cyber supply chain*. Em um segundo nível, a organização deve planejar a execução dessas atividades com marcos bem definidos, além de coletar indicadores que as atividades estão sendo executadas.

E no último nível, os resultados dos indicadores aferidos servem como insumo para a realizar de melhorias nos controles de segurança cibernética. Este nível avançado visa atender o princípio *Zero Trust* "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança". Em síntese, os níveis são expostos no *checklist* abaixo.

- Básico (S.1): Existe um programa de atividades de segurança atuando em aspectos da *cyber supply chain*?
- Intermediário (S.2): Existe um planejamento de execução das atividades com marcos bem definidos ?
  São coletados indicadores da execução das atividades ?
- Avançado (S.3): Os indicadores coletados são utilizados para melhorar o processo continuamente?

3.2.4.2 Conscientização e treinamento (C14)

Conforme discutido na Seção 2.6.1.14, as equipes precisam ser treinadas para conduzir as atividades com o nível de segurança apropriado. Desta forma, em um nível inicial de implementação do controle deve-se estabelecer um programa de treinamentos. Esse programa deve abordar diversos tipos de ameaças internas e externas, assim como esclarecer os papéis e responsabilidades dos agentes envolvidos na *cyber supply chain*.

Em um segundo momento, a organização deve documentar as informações sobre os riscos da *cyber supply chain* e lições aprendidas repassadas durante os treinamentos. E em um estágio mais avançado, esse programa de treinamentos deve ser frequentemente atualizado considerando as tendências identificadas. É interessante que toda a documentação gerada seja de fácil acesso e tenha participação da alta gestão durante a sua criação. Considerando o exposto, seguem os níveis do controle em um formato de *checklist*.

- Básico (S.1): Existe um programa de treinamentos sobre riscos na *cyber supply chain* considerando os diferentes tipos de ameaças e agentes envolvidos ?
- Intermediário (S.2): A organização registra as informações do programa de treinamentos sobre os riscos da *cyber supply chain* ?
- Avançado (S.3): O programa de treinamentos é atualizado continuamente de acordo com tendências identificadas por meio de controles automatizados ?

3.2.4.3 Auditoria e responsabilização (C15)

Com o intuito de proteger a *cyber supply chain*, a organização deve ser capaz de auditar os componentes e serviços oferecidos por terceiros conforme discutido em 2.6.1.15. Essa auditoria deve considerar pelo menos os princípios *Zero Trust* "P1. Todas as fontes de dados e serviços computacionais são considerados recursos", "P5. A organização monitora a integridade e segurança de todos os ativos" e "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança".

No nível básico de implementação desse controle, a organização deve estabelecer uma política de auditoria que é capaz de analisar as ações realizadas nos componentes e serviços ofertados por terceiros. Com esse objetivo, deve-se estabelecer um formato estruturado dos registros que facilite a sua compreensão e processamento. No nível intermediário, esses registros são analisados por meio de técnicas de ciência de dados. E no nível avançado, são implementadas técnicas que garantem o não-repúdio das informações dos componentes e serviços da *cyber supply chain*. Em síntese, segue o *checklist* dos níveis do controle apresentado.

- Básico (S.1): Existe uma política de auditoria considerando ações da *cyber supply chain* ?
  Essas ações são logadas em um formato que possibilita análises futuras?
- Intermediário (S.2): Os *logs* dos eventos coletados são analisados ?
- Avançado (S.3): São implementadas técnicas que garantem o não-repúdio das informações da *cyber supply chain* ?

3.2.4.4 Integridade das informações (C16)

A garantia da integridade das informações é fundamental para a proteção dos componentes e serviços da *cyber supply chain*. Desta forma, a organização deve implementar controles dessa natureza respeitando pelo menos os princípios *Zero Trust* "P2. Toda comunicação é protegida independente de sua localização" e "P5. A organização monitora a integridade e segurança de todos os ativos".

Em um primeiro momento, a organização deve estabelecer uma política de integridade das informações dos componentes e serviços prestados por terceiros. E a seguir, deve-se implementar mecanismos que sejam eficientes mesmo na presença de ameaças internas. E por fim em um estágio mais avançado, deve-se automatizar verificações dos mecanismos que possibilitam o monitoramento contínuo e a identificação de falhas. Esses níveis estão expostos a seguir em formato de *checklist*.

- Básico (S.1): Existe uma política de integridade das informações da *cyber supply chain* ?
- Intermediário (S.2): Os mecanismos de integridade das informações levam em consideração ameaças internas como equipamentos infectados por *malwares*?
- Avançado (S.3): Falhas nos mecanismos de integridade das informações são reconhecidas e tratadas em tempo real?

É realizado um monitoramento contínuo com alertas tempestivos em caso de identificação de violações de segurança?

3.2.4.5 Planejamento (C17)

O controle de planejamento aqui proposto tem o intuito de rastrear a evolução das políticas de segurança cibernética relacionadas à *cyber supply chain*. Desta forma, ao implementar esse controle a organização seria capaz de detalhar o estado atual e o futuro das políticas, como se fosse um mapeamento do processo atual (AS-IS) e o desenho do processo futuro (TO-BE). Considerando que o desenho futuro deve observar os princípios *Zero Trust* enunciados nas Seções 2.4.1 e 3.1.

No nível básico de implementação desse controle, a organização deve estabelecer uma política de atualização das normas de segurança sobre *cyber supply chain*. No nível intermediário, essas normas devem ser revistas para verificar se estão seguindo os princípios *Zero Trust*. E no nível avançado, essa política é atualizada por meio de indicadores obtidos dos controles automatizados. A seguir segue um resumo desses níveis em um formato de *checklist*.

- Básico (S.1): Existe uma política de atualização das normas de segurança referentes a *cyber supply chain* ?
- Intermediário (S.2): As regras das políticas são atualizadas utilizando princípios *Zero Trust* ?
- Avançado (S.3): A política de atualização de normas recebe insumos de controles automatizados?

3.2.5 Aplicação (D5)

O último domínio visa proteger as aplicações por meio do uso de configurações seguras e monitoramento em tempo real. Os controles agrupados nesse domínio são aquisição de sistemas e serviços, resposta a incidentes, e avaliação de riscos. A tabela 3.5 mostra os controles do domínio "Aplicação (D5)".

3.2.5.1 Aquisição de sistemas e serviços (C18)

O controle referente à aquisição de sistemas e serviços é primordial na proteção da *cyber supply chain*. O tema desse controle já foi discutido na Seção 2.6.1.18 e de maneira sucinta aborda políticas e procedimentos para a aquisição de sistemas e serviços de terceiros. Segundo a abordagem *Zero Trust*, ao se incorporar um componente ou serviço em seu ambiente deve ser feita uma revisão completa das relações de confiança do cliente com o fornecedor e devem ser observados pelo menos os princípios "P1. Todas as fontes de dados e serviços computacionais são considerados recursos", "P3. O acesso aos recursos individuais da organização é concedido para cada sessão", "P5. A organização monitora a integridade e segurança de todos os ativos" e "P6. Toda autenticação e autorização de recursos é dinâmica e estritamente aplicada antes que o acesso seja concedido".

No primeiro estágio de implementação, a organização deve estabelecer uma política de aquisição de sistemas e serviços considerando os componentes e serviços fornecidos por terceiros, além de observar os

Tabela 3.4: Os controles propostos do domínio "Governança e dados (D4)" organizados por domínios e estágios.

Domínio e controles\Estágios		Básico (S.1)	Intermediário (S.2)	Avançado (S.3)
Governança e dados (D4)	**Gerenciamento de programa (C13)**	Existe um programa de atividades de segurança atuando em aspectos da *cyber supply chain*?	Existe um planejamento de execução das atividades com marcos bem definidos ? São coletados indicadores da execução das atividades ?	Os indicadores coletados são utilizados para melhorar o processo continuamente?
	Conscientização e treinamento (C14)	Existe um programa de treinamentos sobre riscos na *cyber supply chain* considerando os diferentes tipos de ameaças e agentes envolvidos ?	A organização registra as informações do programa de treinamentos sobre os riscos da *cyber supply chain* ?	O programa de treinamentos é atualizado continuamente de acordo com tendências identificadas por meio de controles automatizados ?
	Auditoria e responsabilização (C15)	Existe uma política de auditoria considerando ações da *cyber supply chain* ? Essas ações são logadas em um formato que possibilita análises futuras?	Os logs dos eventos coletados são analisados ?	São implementadas técnicas que garantem o não-repúdio das informações da *cyber supply chain* ?
	Integridade das informações (C16)	Existe uma política de integridade das informações da *cyber supply chain* ?	Os mecanismos de integridade das informações levam em consideração ameaças internas como equipamentos infectados por *malwares*?	Falhas nos mecanismos de integridade das informações são reconhecidas e tratadas em tempo real? É realizado um monitoramento contínuo com alertas tempestivos em caso de identificação de violações de segurança?
	Planejamento (C17)	Existe uma política de atualização das normas de segurança referentes a *cyber supply chain* ?	As regras das políticas são atualizadas utilizando princípios *Zero Trust* ?	A política de atualização de normas recebe insumos de controles automatizados?

princípios *Zero Trust* elencados acima. No segundo estágio, deve ser realizada a gerência de configuração dos sistemas e serviços críticos adquiridos de terceiros. E no último estágio, deve-se atualizar frequentemente os mecanismos de proteção utilizando técnicas de ciência de dados e os conceitos de DevSecOps. Por fim, esses níveis do controles são apresentados no formato de um *checklist*.

- Básico (S.1): Existe uma política de aquisição de sistemas e serviços que considera aspectos de segurança em uma *cyber supply chain* ?
- Intermediário (S.2): Existe uma gerência de configuração dos sistemas e serviços críticos ?
  São segregados os papéis com conflito de interesse ?
- Avançado (S.3): Os mecanismos de proteção da política de aquisição de sistemas e serviços são atualizados dinamicamente ?

3.2.5.2 Resposta a incidentes (C19)

Os clientes e fornecedores de componentes e serviços devem implementar uma série de controles relacionados à resposta a incidentes conforme discutido em 2.6.1.19. Esses controles devem observar no mínimo os princípios *Zero Trust* "P1. Todas as fontes de dados e serviços computacionais são considerados recursos" e "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança".

No nível básico de implementação dos controles dessa natureza, a organização deve estabelecer um plano de resposta a incidentes considerando os componentes e serviços ofertados por terceiros. No nível intermediário, deve-se implementar mecanismos capazes de compartilhar informações sobre os incidentes da *cyber supply chain* facilitando a comunicação entre fornecedores e clientes. Desta forma, um fornecedor seria capaz de informar a todos os clientes afetados por uma vulnerabilidade presente em um de seus componentes ou serviços. E em um nível mais avançado, esse plano de resposta a incidentes é atualizado frequentemente por meio de técnicas de ciências de dados e DevSecOps permitindo uma melhora contínua. Resumidamente, seguem os níveis desses controles no formato de um *checklist*.

- Básico (S.1): Existe um plano de resposta a incidentes na *cyber supply chain* ?
- Intermediário (S.2): Existe um compartilhamento de informações de incidentes na *cyber supply chain* ?
- Avançado (S.3): O plano de resposta a incidentes é atualizado dinamicamente permitindo a tomada de decisões em tempo real ?

3.2.5.3 Avaliação de riscos (C20)

No último controle, é realizada uma avaliação dos riscos operacionais resultantes da utilização de componentes e serviços de terceiros, conforme discutido na Seção 2.6.1.20. Nesse controle devem ser

observados no mínimo os princípios *Zero Trust* "P5. A organização monitora a integridade e segurança de todos os ativos" e "P7. A organização coleta o máximo possível de informações sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua política de segurança".

No primeiro nível de implementação do controle é estabelecida uma política de avaliação dos riscos dos componentes e serviços da *cyber supply chain*. No segundo nível, são realizadas análises proativas e consideradas tendências identificadas por meio de monitoramento e varreduras de vulnerabilidades. E por fim no último nível, mecanismos automatizados por meio de conceitos de DevSecOps atualizam frequentemente os controles de avaliação de riscos da cadeia de fornecimento. Esses níveis desse controle são expostos a seguir no formato de *checklist*.

- Básico (S.1): Existe uma política de avaliação de riscos da *cyber supply chain*?
- Intermediário (S.2): Os componentes da *cyber supply chain* são proativamente analisados em busca por vulnerabilidades?
  Nessa análise são consideradas tendências no monitoramento e varredura das vulnerabilidades?
- Avançado (S.3): Os controles de avaliação de riscos são atualizados frequentemente por meio de mecanismos automatizados ?

3.2.6 Considerações sobre os controles

Os princípios *Zero Trust* aqui apresentados se aplicam à maioria dos controles, exceto quando o princípio prediz a execução de uma atividade que não é necessária para a implementação do mecanismo de proteção. A organização dos controles em domínios não é rígida, é possível classificá-los em mais em um domínio. No entanto, para simplificar a estrutura, a classificação levou em consideração o domínio predominante.

Em boa parte dos controles, no primeiro nível é avaliado se existe algum normativo compatível com os princípios de *Zero Trust* sobre a categoria de riscos aferida. Considerando a existência do normativo, no segundo nível é questionado se é executada alguma boa prática presente em uma arquitetura *Zero Trust*. E por último, no terceiro nível, é avaliado se os mecanismos são atualizados em tempo real, correspondendo a um alto grau de automação e consequentemente um custo de implementação mais elevado.

Também cabe observar que nos riscos relacionados ao controle de acesso, pode-se determinar as permissões por meio das seguintes perguntas, que formam a sigla 5W+3H [68]:

- *What* - Qual aplicação está sendo utilizada para acessar o recurso dentro da superfície protegida ?
- *Where* - Qual é o destino da solicitação de acesso ?
- *When* - Quando o recurso está sendo acessado ?
- *Who* - Quem deveria ter acesso a esse recurso ?

Tabela 3.5: Os controles propostos do domínio "Aplicação (D5)" organizados por domínios e estágios.

Domínios e controles\Estágios		**Básico (S.1)**	**Intermediário (S.2)**	**Avançado (S.3)**
Aplicação (D5)	**Aquisição de sistemas e serviços (C18)**	Existe uma política de aquisição de sistemas e serviços que considera aspectos de segurança em uma *cyber supply chain* ?	Existe uma gerência de configuração dos sistemas e serviços críticos ? São segregados os papéis com conflito de interesse ?	Os mecanismos de proteção da política de aquisição de sistemas e serviços são atualizados dinamicamente ?
	Resposta a incidentes (C19)	Existe um plano de resposta a incidentes na *cyber supply chain* ?	Existe um compartilhamento de informações de incidentes na *cyber supply chain* ?	O plano de resposta a incidentes é atualizado dinamicamente permitindo a tomada de decisões em tempo real ?
	Avaliação de riscos (C20)	Existe uma política de avaliação de riscos da *cyber supply chain*?	Os componentes da *cyber supply chain* são proativamente analisados em busca por vulnerabilidades? Nessa análise são consideradas tendências no monitoramento e varredura das vulnerabilidades?	Os controles de avaliação de riscos são atualizados frequentemente por meio de mecanismos automatizados ?

- *Why* - Por que essa requisição está tentando acessar o recurso dentro da superfície protegida ?
- *How* - Como essa requisição está acessando a área protegida por uma aplicação específica ?
- *How much* - Quanto custa disponibilizar acesso a esses recursos ?
- *How long* - Por quanto tempo será concedido o acesso ?

Caso um dispositivo seja comprometido, a integração proposta garante que os danos serão limitados a um escopo reduzido pré-estabelecido. A integração presume que uma violação é inevitável, desta forma restringe constantemente o acesso apenas ao necessário e procura ativamente atividades maliciosas. A proposta também estimula o uso de automações em *pipelines* DevSecOps com o objetivo de fornecer informações cruciais para análises em tempo real. E por fim, a tabela 3.6 sumariza todos os controles da integração proposta.

3.3 ANÁLISE DE *GAP*

A análise de *gap* tem como objetivo a verificação do panorama atual e a definição de um *roadmap* de melhorias de segurança. Essa etapa avalia o estágio atual de implementação de cada controle. Também é possível indicar que algum controle não se aplica ao contexto organizacional, porém nesse caso deve-se apresentar uma justificativa. Para facilitar a execução dessa análise foi disponibilizado um *checklist* no link.

Após a análise de *gap* de cada componente, é conduzida uma análise global do produto de *software*. Para isso deve-se sobrepor as análises de cada componente de acordo com sua hierarquia. E logo em seguida, verifica-se se uma camada inferior implementa um controle que mitiga um risco identificado em uma camada superior. Análogo ao problema da Torre de Hanoi, no qual em qualquer movimento o disco inferior deve possui um diâmetro maior do que o disco superior.

Para visualizar as análises realizadas é proposta a representação gráfica ilustrada na figura 3.3 . Pode-se identificar oportunidades de melhorias de segurança por meio dos *gaps* encontrados, espaços em branco. E também é possível constatar que alguns componentes podem proteger falhas presentes em outras camadas. Como exemplo, podemos verificar que o componente vermelho implementa controles do domínio "Identidade" que não eram protegidos pelo seu componente superior azul. Uma versão interativa do gráfico está disponível no link.

Outra visualização para a integração de uma arquitetura *Zero Trust* em uma *cyber supply chain* é apresentada em três níveis pelas figuras 3.4 (nível 1), 3.5 (nível 2) e 3.6 (nível 3). Nessa visualização cada componente do SBOM é um círculo. As relações de hierarquia são representadas por camadas. E as cores correspondem aos estágios de implementação dos controles aferidos na análise de *gap*. Uma versão interativa dessa representação pode ser acessada no link.

Tabela 3.6: Os controles propostos organizados por domínios e estágios.

Domínios e controles\Estágios		**Básico (S.1)**	**Intermediário (S.2)**	**Avançado (S.3)**
Infraestrutura e redes (D1)	**Controle de acesso (C1)**	Existe uma política de acesso que considera aspectos da *cyber supply chain* ?	O controle de acesso é executado em cada sessão ? As permissões de acesso são revisadas periodicamente ? É concedido o mínimo acesso necessário para que os usuários possam executar suas atividades ? As permissões de acesso são segregadas ? É realizada uma microsegmentação da rede ?	O controle de acesso é baseado em uma política atualizada dinamicamente que permite a tomada de decisões em tempo real ? É possível rastrear todas as ações dos usuários ?
	Gerenciamento de configuração (C2)	Existe uma política definida sobre como realizar o gerenciamento de configuração da *cyber supply chain* ? Existem procedimentos sobre como adicionar ou remover componentes do ambiente organizacional ?	Existe uma linha de base da configuração da *cyber supply chain* ? Existe um controle de mudanças de configuração estabelecido ?	O controle de mudanças de configuração é automatizado ? É possível analisar dinamicamente impactos de maneira a permitir a tomada de decisões em tempo real ?
	Manutenção (C3)	Existem políticas e procedimentos para a manutenção da *cyber supply chain* ?	As informações sobre as manutenções são compartilhadas levando em consideração aspectos de uma arquitetura *Zero Trust* ?	As atividades de manutenção da *cyber supply chain* são automatizadas ? As manutenções são continuamente monitoradas ?
Identidade (D2)	**Proteção dos sistemas e comunicações (C4)**	Existe uma política de proteção das comunicações utilizadas na *cyber supply chain* ?	A organização protege suas fronteiras considerando ameaças internas ? As comunicações são protegidas em diversas camadas heterogêneas considerando possíveis falhas em alguns mecanismos ?	Os mecanismos de proteção das comunicação são monitorados e adaptados continuamente?
	Autenticação (C5)	Existe uma política de autenticação na *cyber supply chain* ?	É realizada a gestão da identidade na *cyber supply chain* ? São utilizados múltiplos fatores de autenticação ?	A autenticação é baseada em uma política atualizada dinamicamente permitindo decisões em tempo real ?
	Segurança de pessoal (C6)	Existe uma política de segurança de pessoal considerando aspectos de segurança da *cyber supply chain* ?	É realizada uma investigação social na contratação de empregados que irão atuar em componentes críticos da *cyber supply chain* ? Existe um monitoramento do comportamento de pessoas que atuam na infraestrutura crítica ?	Os mecanismos de verificação do cumprimento da política de segurança de pessoal são monitorados e aprimorados continuamente ?
	Processamento de informações pessoais (C7)	Existe uma política de processamento de informações pessoais aplicada na *cyber supply chain* ?	Os dados pessoais são manipulados de maneira adequada considerando tanto ameaças internas quanto externas à organização ?	Os mecanismos de proteção de dados pessoais são atualizados constantemente ?
Dispositivo (D3)	**Gerenciamento de riscos da *cyber supply chain* (C8)**	Existe uma política de gerenciamento dos riscos da *cyber supply chain* ?	Existe um inventário dos fornecedores e é possível verificar a autenticidade dos componentes da *cyber supply chain* ?	O plano de gerenciamento dos riscos da *cyber supply chain* é atualizado frequentemente baseado em insumos coletados automaticamente ?
	Avaliação, autorização e monitoramento (C9)	A política de segurança da informação da organização incorpora aspectos de avaliação da *cyber supply chain* ?	Existe um plano de ações e marcos de avaliação da *cyber supply chain* ?	É realizado um monitoramento contínuo analisando tendências de forma a possibilitar a tomada de decisão em tempo real ?
	Plano de contingência (C10)	Existe um plano de contingência para a *cyber supply chain* ?	Os ativos críticos da *cyber supply chain* são identificados ?	A organização é capaz de prestar serviços alternativos considerando aspectos de uma arquitetura *Zero Trust* ?
	Proteção física e de ambiente (C11)	Existe uma política de proteção física e de ambiente ?	O acesso físico é segregado por papéis ? Existe uma proteção contra modificações físicas?	Os ativos são monitorados e rastreados continuamente ?
	Proteção de mídias (C12)	Existe uma política de proteção de mídias utilizadas na *cyber supply chain* ? A organização emprega criptografia na proteção de dados sensíveis nas mídias ?	A organização sanitiza as mídias ?	Existe um monitoramento contínuo das mídias que possibilita a tomada de decisões em tempo real ?
	Gerenciamento de programa (C13)	Existe um programa de atividades de segurança atuando em aspectos da *cyber supply chain*?	Existe um planejamento de execução das atividades com marcos bem definidos ? São coletados indicadores da execução das atividades ?	Os indicadores coletados são utilizados para melhorar o processo continuamente?
Governança e dados (D4)	**Conscientização e treinamento (C14)**	Existe um programa de treinamentos sobre riscos na *cyber supply chain* considerando os diferentes tipos de ameaças e agentes envolvidos ?	A organização registra as informações do programa de treinamentos sobre os riscos da *cyber supply chain* ?	O programa de treinamentos é atualizado continuamente de acordo com tendências identificadas por meio de controles automatizados ?
	Auditoria e responsabilização (C15)	Existe uma política de auditoria considerando ações da *cyber supply chain* ? Essas ações são logadas em um formato que possibilita análises futuras?	Os logs dos eventos coletados são analisados ?	São implementadas técnicas que garantem o não-repúdio das informações da *cyber supply chain* ?
	Integridade das informações (C16)	Existe uma política de integridade das informações da *cyber supply chain* ?	Os mecanismos de integridade das informações levam em consideração ameaças internas como equipamentos infectados por *malwares*?	Falhas nos mecanismos de integridade das informações são reconhecidas e tratadas em tempo real? É realizado um monitoramento contínuo com alertas tempestivos em caso de identificação de violações de segurança?
	Planejamento (C17)	Existe uma política de atualização das normas de segurança referentes a *cyber supply chain* ?	As regras das políticas são atualizadas utilizando princípios *Zero Trust* ?	A política de atualização de normas recebe insumos de controles automatizados?
Aplicação (D5)	**Aquisição de sistemas e serviços (C18)**	Existe uma política de aquisição de sistemas e serviços que considera aspectos de segurança em uma *cyber supply chain* ?	Existe uma gerência de configuração dos sistemas e serviços críticos ? São segregados os papéis com conflito de interesse ?	Os mecanismos de proteção da política de aquisição de sistemas e serviços são atualizados dinamicamente ?
	Resposta a incidentes (C19)	Existe um plano de resposta a incidentes na *cyber supply chain* ?	Existe um compartilhamento de informações de incidentes na *cyber supply chain* ?	O plano de resposta a incidentes é atualizado dinamicamente permitindo a tomada de decisões em tempo real ?
	Avaliação de riscos (C20)	Existe uma política de avaliação de riscos da *cyber supply chain*?	Os componentes da *cyber supply chain* são proativamente analisados em busca por vulnerabilidades? Nessa análise são consideradas tendências no monitoramento e varredura das vulnerabilidades?	Os controles de avaliação de riscos são atualizados frequentemente por meio de mecanismos automatizados ?

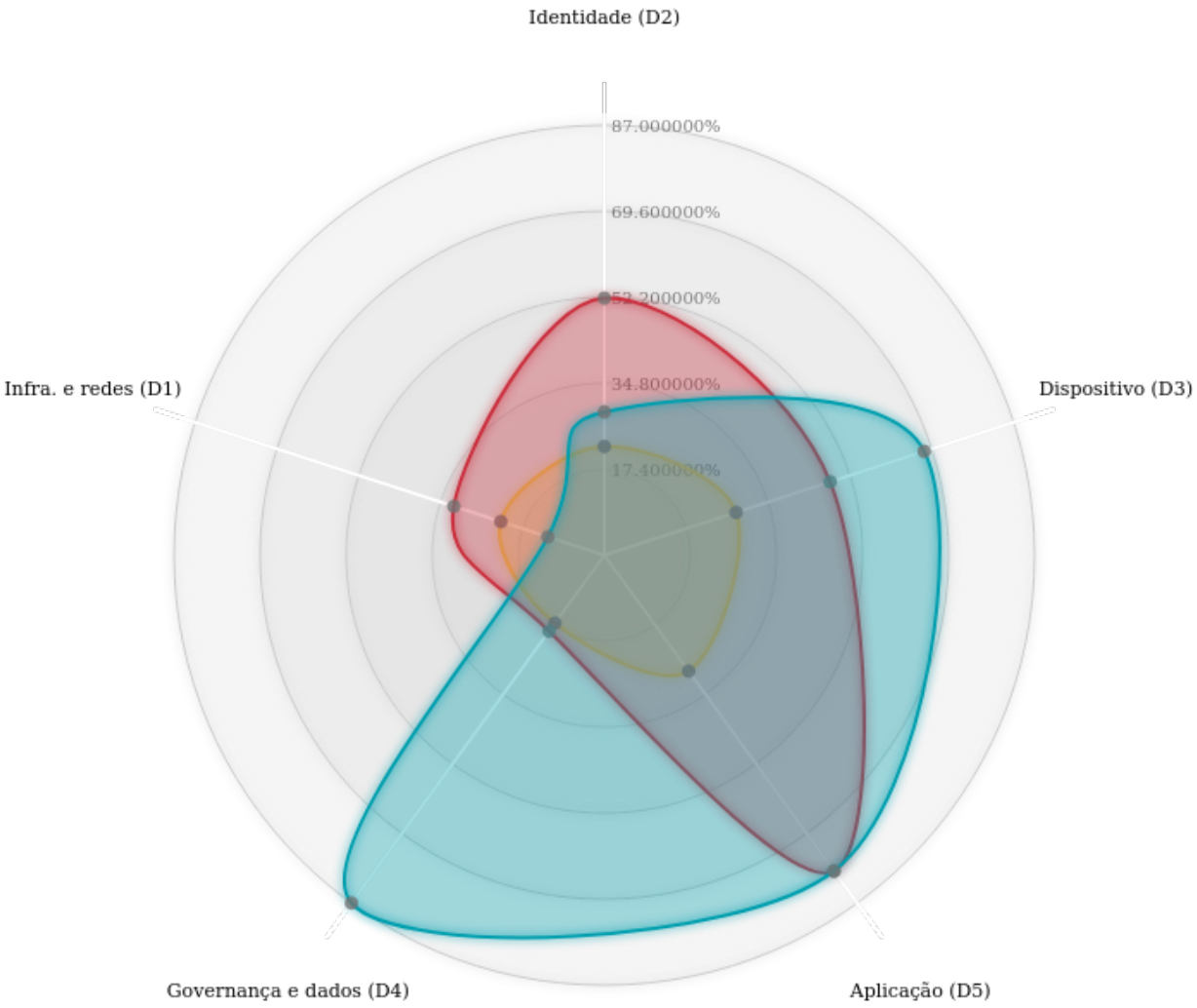

Figura 3.3: Uma análise de *gap* para fins de ilustração

3.4 DESENHO DO *ROADMAP*

O desenho do *roadmap* de melhorias de segurança deve ser baseado na análise de *gap*. É interessante que essa melhoria seja gradual para diminuir o impacto nas operações da organização. Portanto, é recomendado que se implemente controles dos estágios básico e intermediário antes de se investir no nível avançado, mais custoso, conforme discussão realizada por Z. A. Collier and J. Sarkis [31]. Assim, levando em consideração esse critério é possível priorizar a implementação dos controles.

Figura 3.4: Primeiro nível de uma representação visual do SBOM demonstrando uma integração de uma arquitetura *Zero Trust* em uma *cyber supply chain*

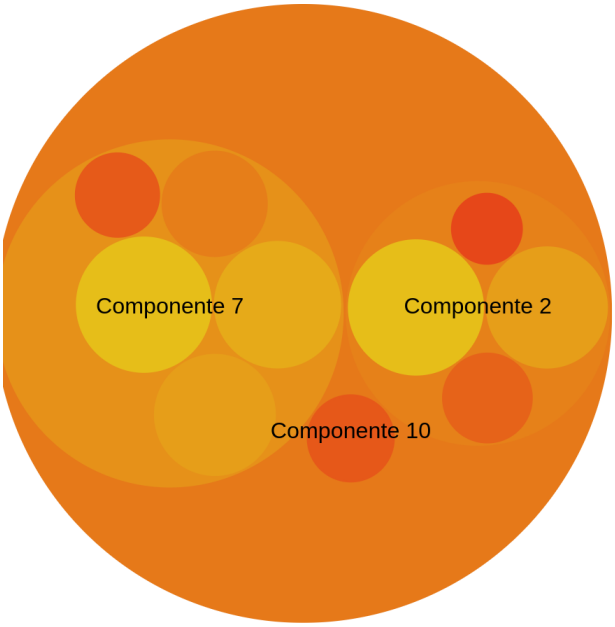

Figura 3.5: Segundo nível de uma representação visual do SBOM demonstrando uma integração de uma arquitetura *Zero Trust* em uma *cyber supply chain*

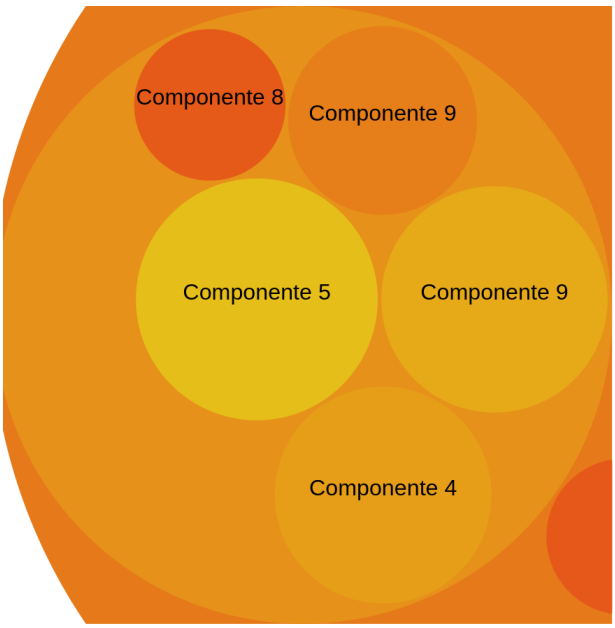

Figura 3.6: Terceiro nível de uma representação visual do SBOM demonstrando uma integração de uma arquitetura *Zero Trust* em uma *cyber supply chain*

3.5 COMPARAÇÃO DA PROPOSTA COM OUTRAS ABORDAGENS

Nas próximas Seções 3.5.1,3.5.2, 3.5.3,3.5.4, 3.5.5 é realizado um comparativo da integração proposta com os trabalhos correlatos identificados no capítulo 2.

3.5.1 Relatório da European Union Agency for Cybersecurity (ENISA)

O relatório da ENISA apresenta uma série de recomendações para proteção da *cyber supply chain*. Nesse estudo, esses controles de segurança são apresentados com um mapeamento de como podem ser incorporados na proposta de integração realizada anteriormente. Cabe destacar que os autores do relatório da ENISA se inspiraram nas normas ISO/IEC 27002, ISO 9001 e ISO 31000 durante a proposta das recomendações.

Os controles propostos pela ENISA são categorizados da seguinte maneira:

- Gerenciamento dos riscos de segurança cibernética;
- Gerenciamento das relações com os fornecedores;
- Desenvolvimento seguro de produtos e serviços;
- Gerenciamento de vulnerabilidades;

O desenvolvimento de sistemas depende de fornecedores de componentes de softwares. Esses componentes diminuem o custo de desenvolvimento e aceleram a entrega do produto final, sendo o reúso de software considerado uma boa prática de programação. Existe até uma metáfora idiomática "reinventar

a roda" considerado um *anti-pattern*, que consiste na criação de uma solução local para um propósito específico em vez de utilizar uma solução aceita globalmente [69].

Uma organização se protege melhor de ataques cibernéticos ao analisar minuciosamente seus fornecedores. Segundo o relatório da ENISA, os fornecedores estão se tornando o elo mais fraco da *cyber supply chain* [6]. Também cabe destacar que cada vez mais os clientes exigem um grau elevado de cibersegurança dos fornecedores, porém não estão dispostos a pagar valores adicionais por esse requisito não-funcional. Além disso, o relatório da ENISA observou que as organizações estão mais conscientes da necessidade de avaliar a maturidade em segurança cibernética dos seus fornecedores e o nível de exposição ao risco que surge da relação entre fornecedor e cliente.

A seguir são apresentados os controles que podem ser adotados por clientes para mitigar os riscos de ataques à *cyber supply chain* elencados no relatório da ENISA.

Os controles relacionados ao gerenciamento de riscos de segurança cibernética são:

- Identificar os fornecedores e os provedores de serviço. Equivale a etapa de identificação dos componentes da *cyber supply chain* da integração proposta;
- Definir os critérios de risco para os diferentes tipos de fornecedores e serviços. A política de gerenciamento de riscos da *cyber supply chain* deve definir esses critérios no controle "Gerenciamento de riscos da *cyber supply chain* (C8)";
- Avaliar os riscos da *cyber supply chain* de acordo com os requisitos de continuidade de negócio da organização. Essa análise deve ser realizada no controle "Plano de contingência (C10)";
- Definir medidas de tratamento de riscos baseadas em boas práticas. Essa definição deve ser inserida na política de gerenciamento de riscos prevista no controle "Gerenciamento de riscos da *cyber supply chain* (C8)";
- O monitoramento de ameaças e riscos da *cyber supply chain* deve ser baseado em fontes internas e externas de informação. Essa diretriz deve ser incluída no controle "Avaliação de riscos (C20)";
- Sensibilizar os empregados da organização sobre os riscos. Essa atividade deve estar presente no controle "Conscientização e treinamento (C14)".

Os controles relacionados ao gerenciamento das relações com os fornecedores são:

- Gerenciamento de fornecedores em todo o ciclo de vida de serviços e produtos. Essa atividade deve ser conduzida no controle "Aquisição de sistemas e serviços (C18)";
- Classificação de ativos e informações que serão compartilhadas com os fornecedores, e definir os procedimentos de permissão de acesso. Esse item está coberto pelo "Controle de acesso (C1)";
- Definir as obrigações dos fornecedores quanto a proteção dos ativos da organização nos seguintes aspectos: compartilhamento de informações, auditoria, continuidade de negócio, segurança de pessoal, tratamento de incidentes nos termos de responsabilidade, obrigações de notificação e procedimentos. Esse tópico inclui atividades dos controles "Segurança de pessoal (C6)", "Plano de contingência (C10)", "Auditoria e responsabilização (C15)".

- Definir os requisitos de segurança de serviços e produtos adquiridos. Esses requisitos são abordados pela política de aquisição de sistemas e serviços presente no décimo sétimo controle "Aquisição de sistemas e serviços".

- Explicitar em contratos com os fornecedores todas as obrigações e requisitos relacionados à segurança da *cyber supply chain*. Essa diretriz deve estar presente no décimo quinto controle "Auditoria e responsabilização".

- Monitorar o desempenho dos serviços e executar as rotinas de auditoria para verificar a aderência aos requisitos de segurança cibernética explicitados em contratos. Essas atividades estão presentes no controle "Auditoria e responsabilização" (C15).

- Receber garantias dos fornecedores e dos prestadores de serviço que nenhum *backdoor* é inserido intencionalmente. Essa garantia deve ser coberta no controle "Auditoria e responsabilização (C15)".

- Assegurar que os requisitos legais são considerados. A política de atualização de normas do controle "Planejamento (C17)" deve considerar esse ponto.

- Definir processos para gerenciar mudanças nos acordos dos fornecedores. Esses processos devem ser definidos na política do controle "Gerenciamento de configuração (C2)".

Cabe frisar que quando um componente de *software* livre é utilizado no produto final, a responsabilização legal é prejudicada, pois como esse componente foi obtido de forma gratuita, não existe uma relação de consumo. Portanto, não se aplicam as obrigações dispostas no Código de Defesa do Consumidor [70].

O relatório da ENISA elenca os controles abaixo sobre o desenvolvimento seguro de produtos e serviços que poderiam ser implementados pelos fornecedores. Destaca-se que esses controles são categorizados no domínio "DevSecOps e ciência de dados (D6)" da integração proposta.

- Garantir que a infraestrutura utilizada para projetar, desenvolver, manter e entregar produtos, componentes e serviços siga as boas práticas de cibersegurança, por exemplo, a norma ISO/IEC 27001.

- Implementar um processo de desenvolvimento de produtos, manutenção e de suporte que se baseia em boas práticas de mercado. Esses processos poderiam ser automatizados via um *pipeline* "DevSecOps" de maneira a diminuir o tempo de entrega dos produtos de *software* e garantir a integridade dos artefatos.

- Implementar um processo de engenharia seguro que seja consistente com as práticas de segurança comumente aceitas, por exemplo, o padrão internacional *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers* conhecido pela sigla "IEC 62443-2-4".

- Considerar a aplicabilidade de requisitos técnicos com base na categoria dos produtos e seus riscos. O padrão "IEC 62443-2-4" provê um amplo conjunto de requisitos de segurança que são categorizados em: aplicações, dispositivos embarcados, *hosts* e dispositivos de redes.

- Oferecer declarações de conformidade aos clientes para normas conhecidas, por exemplo ISO/IEC 27001. Além de garantir, na medida do possível, a integridade e a origem do *software* livre utilizado em qualquer parte do seu componente.
- Definir objetivos de qualidade, por exemplo, quantidade de defeitos, vulnerabilidades identificadas, ou problemas externos relatados. Assim como utilizar essas métricas para melhorar a qualidade do componente.
- Manter dados precisos e atualizados sobre a origem dos componentes de software e sobre os controles aplicados no processo de desenvolvimento. Essa necessidade demonstra a importância da existência de uma frente de ciência de dados aplicada ao desenvolvimento seguro.
- Executar regularmente auditorias para garantir que as medidas acima estão sendo cumpridas.

Cabe observar que o relatório da ENISA afirma que o processo de engenharia seguro deve incluir o uso de ferramentas automatizadas para manter a confiança no código da *cyber supply chain*. De forma a assegurar a integridade do código e ser capaz de checar vulnerabilidades conhecidas. Esse tipo de automação se enquadra bem no uso de uma esteira de desenvolvimento baseada nos conceitos de DevSecOps. Assim como as práticas de desenvolvimento seguro sugeridas pelo Relatório da ENISA que englobam os seguintes pontos:

- Segregação dos ambientes de desenvolvimento, homologação e produção;
- Auditoria das relações de confiança. Esse tipo de revisão das relações de confiança é um dos pontos fundamentais de uma abordagem *Zero Trust*;
- Estabelecimento de múltiplos fatores de autenticação, autenticação baseada em risco, e acesso limitado em toda a organização. Boa prática que deve ser conduzida no "Controle de acesso (C1)";
- Cifração de dados sensíveis. A utilização de criptografia adequada para proteção de dados sensíveis é prevista no controle "Proteção dos sistemas e comunicações (C4)"de forma a proteger informações pessoais de acordo com o previsto na LGPD e também devem ser utilizadas técnicas de anonimização quando aplicável;
- Monitoramento de operações com emissão de alertas. Além da resposta a incidentes de segurança cibernética. Atividades previstas no controle "Resposta a incidentes (C19)".

Os fornecedores também podem implementar boas práticas no gerenciamento de vulnerabilidades. O relatório da ENISA elenca as seguintes práticas:

- Monitoramento de vulnerabilidades reportadas por fontes internas e externas. Esse monitoramento também deve abranger componentes de terceiros. Na proposta apresentada nesse trabalho esse monitoramento deve ser conduzido com o auxílio de ferramentas que conseguem analisar o SBOM. Um exemplo de ferramenta de *Software Composition Analysis* (SCA) é a *dependency track* da OWASP;
- Analisar o risco das vulnerabilidades utilizando um sistema de pontuação, como o *Common Vulnerability Scoring System* (CVSS)[71]. Essa classificação de riscos deve ser realizada no controle "Avaliação de riscos (C20)".

- Definição de uma política de tratamento das vulnerabilidades identificadas de acordo com o nível do risco apresentado. Essa orientação deve estar presente na política de gerenciamento de riscos do controle "Gerenciamento de riscos da *cyber supply chain* (C8)".

- Processos para informar os clientes. Esse processo deve ser implementado no compartilhamento de informações de incidentes do controle "Resposta a incidentes (C19)".

- Verificar se as correções de segurança (*patches*) estão de acordo com requisitos de segurança cibernética e são compatíveis com os outros componentes. Essa verificação deve ser baseada no gerenciamento de configuração realizado pelo segundo controle da proposta.

- Implementação de um processo de entrega segura de *patches*. Além do compartilhamento de informações sobre as correções com os clientes. Esse processo pode ser englobado pelo controle "Manutenção (C3)".

- Participar de um programa de divulgação de vulnerabilidades que inclui um processo de denúncia e divulgação. Esse tipo de iniciativa de compartilhamento de informações sobre incidentes deve ser conduzida no controle "Resposta a incidentes (C19)", sendo interessante enaltecer a importância da participação da comunidade na descoberta de vulnerabilidades por meio de programas de recompensas. Esse tipo de programa também é conhecido em inglês pelo termo *bug bounty*.

O relatório da ENISA também aconselha que os fornecedores gerenciem as vulnerabilidades por meio de *patches*. Desta forma, um cliente pode monitorar potenciais vulnerabilidades e receber notificações dos seus fornecedores. Segue uma lista de algumas boas práticas relacionadas ao gerenciamento de *patches*:

- Manter um inventário dos ativos incluindo informações relevantes sobre os *patches*. Esse inventário está previsto no controle "Gerenciamento de configuração (C2)";

- Utilizar fontes de informação para identificar vulnerabilidades técnicas relevantes;

- Avaliar os riscos de vulnerabilidades identificadas e ter uma política de manutenção documentada e implementada. Essa boa prática está relacionada com os controles "Manutenção (C3)" e "Avaliação de riscos (C20)";

- Receber os *patches* apenas de fontes legítimas e testá-los antes de implantá-los. Essa diretriz deve ser respeitada pelas atividades conduzidas pelo controle "Manutenção (C3)";

- Implementar medidas alternativas caso o *patch* não esteja disponível ou não possa ser aplicado. Essas medidas alternativas devem estar previstas nos controles de "Manutenção (C3)" e de "Gerenciamento de riscos da cyber supply chain (C8)";

- Definir procedimentos de *rollback* e medidas efetivas de *backup* e restauração. Esses procedimentos devem ser conduzidos pelo controle "Manutenção (C3)".

3.5.2 Supply chain Levels for Software Artifacts (SLSA)

A iniciativa SLSA do Google foca principalmente na garantia da procedência dos artefatos por meio de uma verificação de autenticidade e integridade. Além disso, apresenta alguns controles relacionados à rastreabilidade do código-fonte e à segregação de deveres da equipe de desenvolvimento. A integração proposta pode incorporar algumas abordagens apresentadas no SLSA. Mais especificamente o domínio "DevSecOps e ciência de dados (D6)" pode implementar controles dessa natureza em um etapa do *pipeline* de desenvolvimento capaz de verificar a assinatura digital dos artefatos e auditar a procedência dos artefatos.

3.5.3 OWASP Top 10 CI/CD Security Risks

Os riscos elencados pela OWASP são tratados pelo domínio "DevSecOps e ciência de dados (D6)" por meio da implementação de controles de automação da esteira de desenvolvimento. Esses controles devem controlar adequadamente a entrega dos artefatos. E também ser capazes de controlar o acesso ao *pipeline*. Além de validar apropriadamente a integridade dos artefatos e dar visibilidade aos *logs* de compilação. Um papel importante de uma esteira de integração contínua é permitir que seja realizado um processo de compilação hermético conforme descrito na seção 2.5.6.1.

3.5.4 Guia de segurança da software supply chain do Center of Internet Security (CIS)

O Guia do CIS deve ter suas práticas implementadas em boa parte pelo domínio "DevSecOps e ciência de dados (D6)". Principalmente, as atividades relacionadas ao código-fonte, *pipeline* de desenvolvimento, verificação de dependências, artefatos e entrega contínua. Percebe-se grande similaridade entre a abordagem do guia do CIS e a iniciativa do Google (SLSA) devido ao foco principal na verificação da procedência dos artefatos. Um ponto de diferença dessas duas abordagens e a integração proposta é que o trabalho aqui apresentado possui uma visão mais ampla da *cyber supply chain* não focando apenas nos artefatos de software.

3.5.5 Recomendações da Cloud Native Computing Foundation (CNCF)

As boas práticas apresentadas nas recomendações da CNCF também estão relacionadas ao domínio "DevSecOps e ciência de dados (D6)". Esse domínio trata exatamente da proteção do código-fonte, do processo de compilação, dos artefatos e da entrega contínua. Um ponto interessante das recomendações da CNCF que não foi detalhado na integração proposta é a utilização da abordagem de *Infrastructure as code* (IaC) com a utilização de *containers*. Essa abordagem apresenta benefícios por melhorar a auditabilidade do ambiente de infraestrutura e facilitar o gerenciamento de configuração. Desta forma, ao se implementar a integração aqui apresentada deve-se adotar essas boas práticas.

3.6 RESUMO DO CAPÍTULO

Nesse capítulo foi apresentada a proposta de integração de controles de segurança baseados nos princípios *Zero Trust* em uma *cyber supply chain*. A proposta de integração é resumida na figura 3.2. Os princípios utilizados como inspiração para a definição dos controles foram expostos na Seção 2.4.1.

Os temas dos controles foram escolhidos baseados na discussão realizada na Seção 2.6.1. E para facilitar a compreensão da proposta, os controles foram organizados em domínios e níveis de implementação conforme discutido em 3.1. Com o intuito de fornecer uma ferramenta de avaliação foi disponibilizado um *checklist* ilustrado pela tabela 3.6.

Após o preenchimento do *checklist* é possível realizar uma análise de *gap* por meio das representações visuais ilustradas nas figuras 3.3, 3.4, 3.5, 3.6. Em seguida, a organização é capaz de desenhar um *roadmap* de melhorias de segurança cibernética para a proteção da *cyber supply chain*. E por fim, é apresentado um comparativo dos trabalhos correlatos com a integração proposta nesse capítulo resumido por meio da tabela 3.7.

Tabela 3.7: Comparação dos trabalhos correlatos com a integração proposta nesse capítulo.

Domínios e controles \ estudos		ENISA	SLSA	OWASP	CIS	CNCF	Integração proposta
Infraestrutura e redes (D1)	Controle de acesso (C1)	✓	✓	✓	✓	✓	✓
	Gerenciamento de configuração (C2)		✓	✓	✓	✓	✓
	Manutenção (C3)	✓					✓
	Proteção dos sistemas e comunicações (C4)						✓
Identidade (D2)	Autenticação (C5)	✓	✓	✓	✓	✓	✓
	Segurança de pessoal (C6)	✓					✓
	Processamento de informações pessoais (C7)						✓
	Gerenciamento de riscos da *cyber supply chain* (C8)						✓
Dispositivo (D3)	Avaliação, autorização e monitoramento (C9)						✓
	Plano de contingência (C10)	✓					✓
	Proteção física e de ambiente (C11)		✓				✓
	Proteção de mídias (C12)						✓
Governança e dados (D4)	Gerenciamento de programa (C13)						✓
	Conscientização e treinamento (C14)						✓
	Auditoria e responsabilização (C15)	✓		✓	✓	✓	✓
	Integridade das informações (C16)						✓
	Planejamento (C17)						✓
Aplicação (D5)	Aquisição de sistemas e serviços (C18)						✓
	Resposta a incidentes (C19)						✓
	Avaliação de riscos (C20)						✓

4 ESTUDOS DE CASO

Com o intuito de obter resultados práticos acerca da integração proposta e melhor compreender sua capacidade de aplicação foram elaborados três cenários baseados em ataques recentes reais que exploraram a *cyber supply chain* de infraestruturas críticas. Para cada cenário é feita uma breve explicação do incidente ocorrido e após isso são demonstradas falhas nas famílias de controles adotadas neste trabalho.

O primeiro cenário aborda o ataque conhecido como "sunburst". Esse incidente foi escolhido devido à quantidade de organizações impactadas e pela sua sofisticação. Considerado por algumas entidades como um dos maiores ataques cibernéticos até o momento [7, 6].

O segundo cenário analisa a vulnerabilidade encontrada na biblioteca *Apache Log4j*. Esse incidente também impactou diversas organizações. E demonstra a importância da checagem de bibliotecas de código aberto.

E por último, o terceiro cenário detalha o ataque ocorrido no sistema de distribuição de óleo "Colonial Pipeline". Esse evento mostra a relevância da proteção da infraestrutura crítica brasileira contra ataques cibernéticos dessa natureza.

Cabe ressaltar que nem todos os detalhes sobre os ataques citados foram divulgados então a análise fica limitada aos dados constantes em relatórios e artigos científicos sobre o assunto. Cabe ressaltar que os dados utilizados para a realização dos estudos de caso foram obtidos de fontes abertas e selecionados visando ilustrar a aplicação da integração proposta.

4.1 CENÁRIO 1 - SUNBURST

Em setembro de 2019, um grupo conseguiu acesso ao ambiente de desenvolvimento da empresa norte-americana SolarWinds, cabe observar que o Mitre atribuiu o ataque ao grupo denominado "APT29" [72] e alguns documentos do governo norte-americano e britânico afirmam que esse grupo é o *Russia's Foreign Intelligence Service* (SVR) [73, 74]. No início, os atacantes injetaram um código de teste no processo de compilação da solução Orion, que possui funcionalidades de monitoramento, análise e gerenciamento da infraestrutura de tecnologia da informação de uma organização de um ponto centralizado [75, 76, 77].

Depois de dois meses, os agentes maliciosos interromperam a inserção de código de teste. E aguardaram por mais três meses para compilar e implantar um *backdoor* na plataforma Orion. Logo em seguida, essa versão infectada da plataforma foi distribuída para os clientes. E estima-se que em maio de 2020 foram iniciados os ataques manuais direcionados aos clientes com a ativação do *malware* denominado "TEARDROP" [78]. Em junho, os atacantes removeram o *backdoor* do ambiente de compilação da SolarWinds, demonstrando uma preocupação em não serem notados. Para facilitar o entendimento das ações descritas acima é apresentada uma linha do tempo dos eventos do ataque "sunburst" na figura 4.2 e um diagrama das etapas do ataque na figura 4.1.

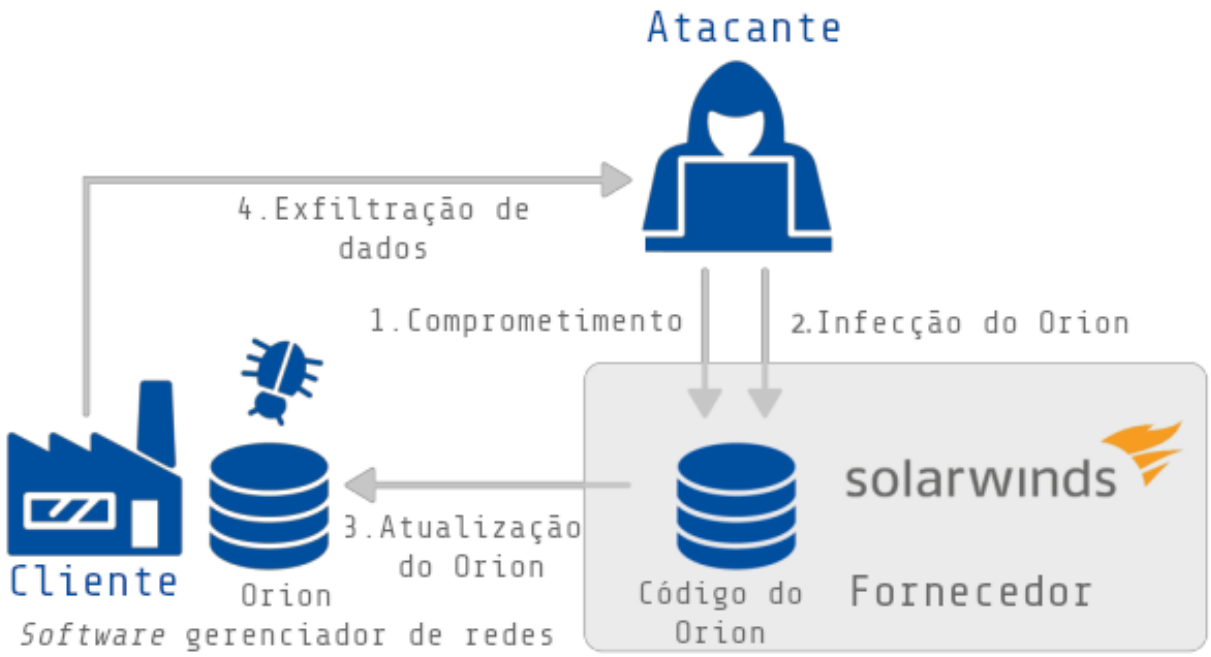

Figura 4.1: Etapas do ataque "sunburst" adaptada do relatório da ENISA [6].

O ataque começou a ser investigado após especialistas da empresa *FireEye* perceberem um comportamento anômalo em suas redes. E uma característica interessante do modo operante dos agentes maliciosos foi a capacidade de se manter oculto, essa característica também é denominada de furtividade. Demonstrando um interesse em manter o acesso de maneira silenciosa por um longo período de tempo, característica de *Advanced Persistent Threats* (APTs). Essa característica é presente em ataques que visam exfiltrar informações de suas vítimas em uma possível operação de espionagem.

Os autores da SLSA defendem que os controles de segurança impostos pelos níveis mais elevados do seu modelo protegeriam uma organização contra ataques similares ao "sunburst". Essa garantia seria decorrente da verificação da autenticidade e da integridade dos artefatos a serem construídos [49].

Antes do ataque "sunburst", alguns consideravam que a identificação de vulnerabilidades nas dependências era atividade apenas de resposabilidade da equipe de desenvolvimento. Porém, os ataques recentes provam que essa abordagem não é mais eficiente. Todo o *pipeline* DevSecOps deve ter sua segurança verificada. E o incidente "sunburst" revelou a importância de se analisar as dependências para garantir sua procedência e sua segurança [80].

Durante a realização desse estudo não foi possível ter acesso ao código da plataforma Orion da SolarWinds e nem a lista de dependências dessa solução num formato de *SBOM*. Desta forma, não foi possível aplicar a parte da integração proposta que trata da decomposição da solução em componentes para analisar a SBOM. Porém, foi viável analisar quais famílias de controles não foram efetivos contra o ataque descrito acima.

Nesse ataque ficou claro que houve uma falha de controle de acesso. Os agentes maliciosos não deveriam ter tido acesso ao código da plataforma Orion e muito menos serem capazes de inserir trechos capazes de realizar acesso remoto, demonstrando uma ineficiência na revisão de código.

Figura 4.2: Linha do tempo do ataque "sunburst" adaptada da documentação da Microsoft [79].

Segundo [7], a origem do ataque pode ter sido uma falha de configuração do repositório no Github que expôs as credenciais de acesso ao servidor da SolarWinds. O repositório deveria estar configurado como privado em vez de público. Esse fato demonstra que houve uma falha na implementação de controles associados ao gerenciamento de configuração.

Também ocorreu um problema ao não se detectar as comunicações indevidas com a central de comando e controle gerenciada pelos agentes maliciosos [7]. Desta forma, podemos afirmar que não existiam controles efetivos da família de proteção dos sistemas e das comunicações.

Em 2019, a empresa SolarWinds já havia passado por um situação constrangedora quando um pes-

quisador da área de segurança cibernética encontrou uma senha fraca "solarwindws123" no repositório de código fonte do servidor de atualização no Github [7]. Esse caso também demonstra que provavelmente ocorreu um problema de autenticação sem o uso recomendado de múltiplos fatores de autenticação.

Segundo a perspectiva de Jelena Mirkovic no documento [81], as modificações realizadas no código da plataforma Orion podem ter sido realizadas por algum empregado da companhia SolarWinds, ou seja, um *insider*. Porém, não foram encontradas outras fontes que confirmassem essa teoria. Então na dúvida não se pode afirmar que houve uma implementação não efetiva dos controles da família de segurança de pessoal.

Cabe ressaltar que a empresa SolarWinds redefiniu o seu ciclo desenvolvimento após o ataque "sunburst". Esse novo ciclo foi documentado no artigo disponível em [82]. Nessa nova abordagem alguns princípios *Zero Trust* foram adotados, como, por exemplo, a organização passou a monitorar a integridade e segurança de todos os ativos. Esse princípio é implementado por um controle de checagem de *hashes* dos artefatos produzidos durante o processo de *build*. Outra melhoria evidente nesse novo processo é a utilização de compilação hermética semelhante ao discutido na Seção 2.5.6.1. E, por fim, cabe destacar uma boa prática adotada que é a microsegmentação do acesso dos desenvolvedores, permitindo manipular apenas o código que está relacionado com as funcionalidade que estão implementando, sem permissão para alterar etapas de validação e segurança do ciclo de desenvolvimento.

4.2 CENÁRIO 2 - APACHE LOG4SHELL/LOG4J

No final de 2021, foram publicadas uma série de vulnerabilidades na biblioteca de gerenciamento de registros Log4j. Sendo uma biblioteca extremamente popular utilizada por mais de trinta e cinco mil pacotes java [83]. Uma das vulnerabilidades descobertas permitia a execução remota de código por meio de uma injeção em uma funcionalidade do *Java Naming and Directory Interface* (JNDI). Sendo que essa funcionalidade era habilitada por padrão em várias versões da biblioteca Log4j, portanto tornando uma ampla gama de sistemas inseguros.

Essa vulnerabilidade ficou conhecida como Log4Shell e trouxe basicamente dois problemas críticos para a comunidade de segurança cibernética. O primeiro deles foi que o código utilizado no ataque se tornou público tornando fácil a condução do ataque, além disso foi possível automatizar o ataque para ser conduzido remotamente, desta forma foi possível observar uma quantidade massiva de ataques dessa natureza nos dias posteriores a publicação da vulnerabilidade [84]. E o segundo problema foi ter revelado a dificuldade das organizações em rastrear as dependências de *software* utilizadas em seus produtos ou serviços. As equipes responsáveis precisavam das informações sobre as dependências para corrigir os softwares de maneira tempestiva.

O Google conduziu algumas análises para facilitar a proteção contra essa vulnerabilidade. Em um dos estudos foi observado que mais de oito porcento dos pacotes observados do repositório central do Maven foram impactados pela vulnerabilidade Log4Shell [85]. Durante as análises foram consideradas dependências diretas e indiretas, a figura 4.3 ilustra a diferença entre os dois tipos de dependências. Pela contagem feita pela equipe do Google mais de sete mil artefatos possuíam dependência direta em um componentes da biblioteca Log4j com uma versão vulnerável. Sendo que a maioria dos artefatos identificados

como vulnerável era em decorrência de uma dependência indireta, ou seja a biblioteca Log4j não constava explicitamente como uma dependência, porém era herdada por meio de uma dependência transitiva.

Outro ponto interessante a ser observado é a velocidade da correção dessas vulnerabilidades nesses artefatos afetados. Em um primeiro momento, pode parecer simples a mera atualização da dependência da biblioteca do Log4j para uma versão com o *path* de segurança. Porém, de uma maneira geral mudanças de versões em dependências podem impactar outras funcionalidades e é difícil dimensionar suas consequências. Adicionalmente, muitos projetos de código aberto contam apenas com trabalho voluntário para sua manutenção. Assim, vulnerabilidades como esta analisada podem perdurar durante vários anos em bibliotecas de *software* utilizadas na *cyber suppy chain* de infraestruturas críticas.

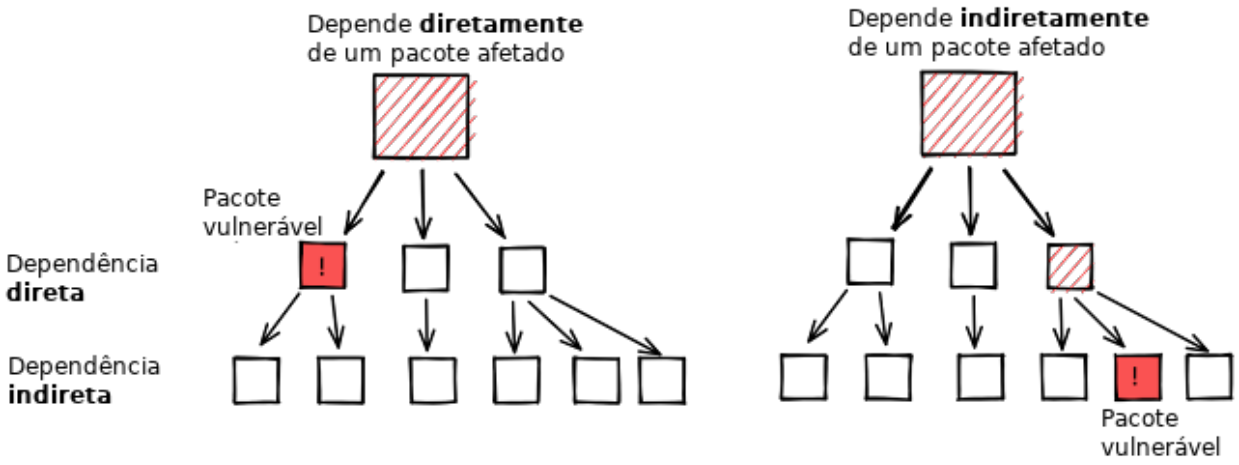

Figura 4.3: Diferença entre dependências diretas e indiretas. Adaptado da análise do Google sobre os impactos da vulnerabilidade Log4Shell [85].

Esse cenário demonstra o potencial impacto da descoberta de uma vulnerabilidade crítica em uma biblioteca de código aberto amplamente utilizada em diversos sistemas em diferentes organizações espalhadas pelo mundo. Outro ponto preocupante nesse caso é que pelo fato da biblioteca ser de código aberto qualquer desenvolvedor pode tentar inserir código malicioso e caso não seja feita uma revisão de código efetiva, esse código malicioso pode ser utilizado em ambiente de produção por várias organizações, sendo essa uma estratégia já exposta na Seção 2.5.3.

Nesse ataque pode-se observar falhas nas seguintes famílias de controles: Controle de acesso, proteção dos sistemas e comunicações, autenticação, aquisição de sistemas e serviços. Uma abordagem que pode proteger de situações similares seria utilizar de princípios de *Zero Trust* que forçam com que sejam revistas as relações de confiança. Desta forma, as dependências utilizadas pelos produtos de *software* precisariam ser analisados e não existiria a possibilidade de se herdar a confiança de um componente pelo fato de já utilizar um outro componente do mesmo fornecedor, ou seja, não ter uma confiança implícita.

4.3 CENÁRIO 3 - COLONIAL PIPELINE

Em maio de 2021, ocorreu um ataque cibernético contra a empresa norte-americana Colonial Pipeline responsável pela distribuição de aproximadamente metade do combustível da costa leste dos Estados Unidos [86, 87]. Esse ataque acarretou uma interrupção dos dutos da organização levando a um estado de emergência devido a falta de combustível. Tanto pessoas físicas quanto pessoas jurídicas precisaram buscar alternativas para conseguir continuar exercendo suas atividades normalmente. Nesse incidente os agentes maliciosos efetuaram um sequestro dos dados e solicitaram um recompensa para a operação da organização voltasse a regularidade, essa técnica também é conhecida em inglês por *ransomware*.

O *Federal Bureau of Investigation* (FBI) atribuiu esse ataque ao grupo DarkSide [88]. Esse grupo possui uma característica curiosa, os seus alvos são escolhidos baseados na localização. Durante o ataque algumas configurações de idioma são verificadas para se evitar que países do antigo bloco da União Soviética sejam alvos de *ransomware* [89].

O ataque se originou a partir de uma senha de um empregado exposta em um fórum na *dark web*. A senha vazada permitia acesso remoto a rede do grupo responsável pela administração da Colonial Pipeline. Na manhã do dia 7 de maio um empregado da organização observou uma nota pedindo uma recompensa em troca dos dados de seu computador e logo em seguida toda a rede da organização já estava comprometida. A falta de um mecanismo de autenticação forte utilizando múltiplos fatores de autenticação evidencia a ineficácia da família de controles relacionadas à autenticação.

Durante a investigação do incidente, percebeu-se que o agente malicioso teve acesso apenas aos sistema de cobrança da organização. Desta forma, não houve nenhum dano físico ao sistema de dutos. E pelo fato do fluxo de óleo ter sido interrompido não houve prejuízo com entrega de óleo sem cobrança.

Cabe observar que esse cenário é diferente dos demais, pois não ocorreu um comprometimento de um componente de software da *cyber supply chain* que foi incorporado na organização cliente sem a devida proteção. Pode-se notar que a *supply chain* explorada nesse cenário foi a da prestação de serviço, pois o empregado que teve sua senha exposta deve ter sofrido algum tipo de ataque, possivelmente uma engenharia social ou um *phishing*. Nesse ataque podemos constatar falhas nas famílias de controles relacionadas ao controle de acesso, à segurança de pessoal, conscientização e treinamento, à autenticação e à aquisição de sistemas e serviços.

Outro ataque à infraestrutura crítica notório ocorrido há alguns anos foi o Stuxnet. No começo de 2010, oficiais da agência internacional de energia atômica responsáveis por monitorar o programa de enriquecimento de urânio do governo Iraniano perceberam um comportamento anormal na controladora de uma centrífuga de uma usina nuclear [90]. Nessa ocasião os sistemas *Supervisory Control And Data Acquisition* (SCADA) foram infectados por um *malware* que aumentava a velocidade de rotação da centrífuga diminuindo o tempo de vida de seus equipamentos. Nesse ataque foram utilizados quatro *zero days* demonstrando a sofisticação da operação possivelmente executada por um Estado-nação [90]. Além disso, podemos destacar que a infecção inicial ocorreu por meio de um *pendrive* mostrando uma falha na *cyber supply chain* de serviço que não adotou os procedimentos corretos ao inserir artefatos maliciosos numa rede segregada da internet, esse tipo de rede é conhecida em inglês como *air gap*.

Esse cenário demonstrou a importância da proteção das infraestruturas críticas de uma nação [86]. E

da necessidade da realização de treinamentos de cenários de crise para exercitar as comunicações institucionais entre as principais entidades envolvidas nas prestações de serviços essenciais a nação. Um exemplo de exercício dessa natureza realizado no Brasil é o Guardião Cibernético. Esse evento acontece anualmente e é o maior exercício de defesa cibernética do hemisfério sul. O objetivo desse exercício é justamente criar um ambiente o mais próximo possível do real onde diversos representantes de infraestruturas críticas brasileiras participantes precisam proteger seus sistemas de ataques cibernéticos. Desta forma, melhorando as comunicações institucionais e contribuindo para o crescimento da resiliência cibernética das infraestruturas críticas brasileiras.

4.4 RESUMO DO CAPÍTULO

Durante a realização dos estudos de casos percebeu-se que existe uma dificuldade na aplicação da integração proposta sem o total conhecimento da SBOM das soluções de software comprometidas. Desta forma, a análise conduzida limitou-se a verificação das famílias de controles que não foram efetivas durante os ataques. Comparando os três ataques analisados, nota-se que uma sequência de controles implementados incorretamente permitem que agentes maliciosos comprometam o ambiente da organização. Considerando apenas as famílias de controles que não foram efetivas em cada um dos cenários estudados, conforme tabela 4.1, pode-se observar um ponto em comum, as falhas no controle de acesso. Sendo que o controle de acesso pode ser divido em autenticação e autorização. Pontos primordiais para um gerenciamento de identidade efetivo. Vulnerabilidades dessa natureza podem ser corrigidas por meio de controles baseados em uma abordagem *Zero Trust* como já discutido nas Seções 2.4.1, 2.6.1.5, 2.6.1.1, 3.2.2.1 e 3.2.1.1.

No modelo proposto o acesso possui a granularidade adequada. Ou seja, apenas o dispositivo devidamente autorizado irá realizar o acesso no momento correto. Sendo que essas políticas de acesso são atualizadas dinamicamente baseado na análise dos dados dos usuários e sistemas. Por meio da microsegmentação pode-se particionar os acessos para se evitar movimentos laterais na ocasião de um comprometimento da infraestrutura. E também deve-se utilizar múltiplos fatores de autenticação conforme explicado em 2.6.1.1. Outro fator que também pode ser destacado é a eficiência de técnicas de OSINT para obter senhas de membros de equipes com acesso crítico dentro da organização. Portanto, parece interessante o monitoramento de fontes abertas para se verificar se segredos importantes da organização tenham vazado.

Tabela 4.1: Apenas as famílias de controles que não foram efetivas em cada um dos cenários estudados.

Domínios e controles\Ataques recentes		Sunburst	Apache Log4Shell/Log4j	Colonial Pipeline
Infraestrutura e redes (D1)	Controle de acesso (C1)	✓	✓	✓
	Gerenciamento de configuração (C2)	✓		
	Proteção dos sistemas e comunicações (C4)	✓	✓	
Identidade (D2)	Autenticação (C5)	✓	✓	✓
	Segurança de pessoal (C6)			✓
Governança e dados (D4)	Conscientização e treinamento (C14)			✓
Aplicação (D5)	Aquisição de sistemas e serviços (C18)	✓	✓	

5 CONCLUSÃO

O presente trabalho mostra que uma integração entre *Zero Trust* e *cyber supply chain* é possível. Além de apresentar ferramentas que facilitam essa proposta de integração, juntamente com sua implementação. Por exemplo, o conjunto de controles propostos 3.6 (também disponível no formato de *checklist* no link) e as visualizações sugeridas permitem o desenho de um *roadmap* de melhorias de segurança.

A abordagem *Zero Trust* se mostra interessante na proteção da *suppy chain* por diversos fatores. Um deles é a obrigação da revisão das relações de confiança entre o fornecedor e o cliente. Além disso evita ataques laterais, por solicitar autenticação e verificação da autorização para cada acesso realizado.

Outro ponto importante observado durante a realização deste estudo, é que a análise da segurança da *cyber supply chain* deve ser vista de uma maneira ampla e não apenas focada na integridade de artefatos desenvolvidos internamente pela própria organização. Pois, a *cyber supply chain* de infraestruturas críticas possuem etapas que contém serviços realizados por fornecedores. Apenas para exemplificar o ponto de observação levantado, uma controladora de uma usina nuclear pode ter o seu *firmware* atualizado manualmente por uma equipe prestadora de serviços de manutenção. Desta forma, devem existir mecanismos de responsabilização por meio de contratos com os fornecedores.

Considera-se que o objetivo do estudo foi alcançado. Dado que revisou e comparou as famílias de controles de segurança de uma *cyber supply chain* implementadas pelos principais trabalhos correlatos identificados, conforme exposto nas Seções 2.6.1, 2.6.2 e na tabela 3.7. Este trabalho também forneceu uma proposta de integração de controles baseados em princípios *Zero Trust* para proteção de uma *cyber supply chain*. Essa proposta é representada por um conjunto de controles organizados em domínios e estágios de implementação formatados em um *checklist* descritos na Seção 3.2. Nessa mesma Seção 3.2, os controles são relacionados com os princípios *Zero Trust* que norteiam sua implementação. Os controles são classificados em domínios e em estágios de implementação na tabela 3.6. Na seção 3.3 foi demonstrado uma visualização da mensuração de aderência aos controles que permite o desenho de um *roadmap* de melhorias na segurança de uma *cyber supply chain*. E por fim, foi realizado três estudos de caso de cenários de ataques reais ocorridos recentemente nas seções 4.2, 4.3, 4.2.

Durante o estudo percebeu-se que existe uma lacuna de implementação de controles de segurança para a proteção da *cyber supply chain* nos principais trabalhos correlatos identificados, ilustrada pela tabela 3.7. E após a condução dos estudos de caso ficou claro que existe a necessidade de um foco especial nos controles relacionados ao gerenciamento de identidade, tanto na autenticação quanto na autorização. Sendo esses controles primordiais para a devida proteção da *cyber supply chain*.

5.1 TRABALHOS FUTUROS

Com base nos estudos de caso e conclusões obtidas a partir da realização deste trabalho, são propostos alguns trabalhos futuros a serem explorados em pesquisas subsequentes. Em suma, são sugeridos os

seguintes temas para as próximas pequisas:

- Validação da proposta de integração;
- Análise do custo de implementação dos controles;
- Exploração de mecanismos de automação na esteira *DevSecOps*;
- Aprofundamento nas análises dos dados provenientes das implementações dos controles;
- Prospecção de mecanismos de rastreio de componentes da *cyber supply chain*;

O ferramental apresentado ainda precisa de validação. Desta forma, como sugestão de trabalho futuro poderia ser realizada uma coleta de informações com empresas e órgãos de governo. Essa pesquisa permitiria traçar perfis de implementação dos controles aqui propostos. Assim, possibilitando uma análise minuciosa dos riscos existentes na *cyber supply chain* de vários tipos de organizações.

Também poderia ser detalhado o custo relacionado a implementação de cada nível dos controles de maneira a subsidiar o desenho do *roadmap* de melhorias de segurança. Outro ponto que pode ser investigado é a automação de alguns controles para que seja possível monitorar em tempo real os riscos da *cyber supply chain*. Além de diminuir o esforço da execução de controles manuais. Outro campo a ser explorado é a utilização de algoritmos de aprendizado de máquina para análise de comportamento anormal de componentes da *cyber supply chain*, uma das técnicas que pode ser utilizada para isso é conhecida em inglês pelo termo *User and Entity Behavior Analytics* (UEBA).

Outra frente de pesquisa interessante é a criação de mecanismos para possibilitar o rastreio de componentes com vulnerabilidades, semelhante ao que ocorre na indústria automobilística. Os fabricantes de carros conseguem dimensionar quais veículos são afetados por um lote de peças defeituosas. Da mesma forma, um fornecedor de *software* deveria ser capaz de notificar todos os clientes que utilizam uma versão do componente com vulnerabilidade na *cyber supply chain*.

Em síntese, cabe destacar que nem todos os riscos da *cyber supply chain* podem ser tratados pelos clientes ou fornecedores de *software*. Em específico, *backdoors* não documentados em componentes de *hardware* não podem ser facilmente identificados por verificações de segurança padrão. Além destes, vulnerabilidades *zero day* também continuam sendo um desafio. Além disso, os ataques à *cyber supply chain* podem ser patrocinados por atores estatais. Desta forma, as medidas de proteção devem ser intensificadas para se contrapor a esses desafios.

REFERÊNCIAS BIBLIOGRÁFICAS

1 COUFALÍKOVÁ, A.; KLABAN, I.; ŠLAJS, T. Complex strategy against supply chain attacks. In: *2021 International Conference on Military Technologies (ICMT)*. [S.l.: s.n.], 2021. p. 1–5.

2 INFORMATION and Communications Technology Supply Chain Risk Management. Cybersecurity and Infrastructure Security Agency (CISA), 2022. Disponível em: <https://www.cisa.gov/supply-chain>.

3 ENHANCING the security of the software supply chain to deliver a secure government experience. The United States Government, 2022. Disponível em: <https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/>.

4 GARBIS, J.; CHAPMAN, J. *Zero Trust Security: An Enterprise Guide*. Apress, 2021. ISBN 9781484267011. Disponível em: <https://books.google.com.br/books?id=ofb3zQEACAAJ>.

5 GILMAN, E.; BARTH, D. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. 1st. ed. [S.l.]: O'Reilly Media, Inc., 2017. ISBN 1491962194.

6 CYBERSECURITY and European Union Agency for; VALEROS, V. *ENISA threat landscape for supply chain attacks*. [S.l.]: European Network and Information Security Agency, 2021.

7 DATTA, P. Hannibal at the gates: Cyberwarfare & the solarwinds sunburst hack. *Journal of Information Technology Teaching Cases*, 2021. Disponível em: <https://doi.org/10.1177/2043886921993126>.

8 AMARAL, T. M. S. do; GONDIM, J. J. C. Integrating zero trust in the cyber supply chain security. In: IEEE. *2021 Workshop on Communication Networks and Power Systems (WCNPS)*. [S.l.], 2021. p. 1–6.

9 BEAMON, B. M. Supply chain design and analysis:: Models and methods. *International Journal of Production Economics*, v. 55, n. 3, p. 281–294, 1998. ISSN 0925-5273. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0925527398000796>.

10 EDITOR, C. C. *Advanced persistent threat - glossary: CSRC*. NIST, 2022. Disponível em: <https://csrc.nist.gov/glossary/term/advanced_persistent_threat>.

11 STERN, G. Preparing for the next cyber storm: Are you ready? *Biomed Instrum Technol.*, 53(6), p. 412–419, 2019.

12 MARTIN, R. A. Visibility & control: Addressing supply chain challenges to trustworthy software-enabled things. In: *2020 IEEE Systems Security Symposium (SSS)*. [S.l.: s.n.], 2020. p. 1–4.

13 CADARIU, M.; BOUWERS, E.; VISSER, J.; DEURSEN, A. van. Tracking known security vulnerabilities in proprietary software systems. In: *2015 IEEE 22nd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*. [S.l.: s.n.], 2015. p. 516–519.

14 THE Decentralized Package Network. 2022. Disponível em: <https://pyrsia.io/>.

15 OPEN source insights. 2022. Disponível em: <https://deps.dev/>.

16 2022 Open source security and analysis report. 2022. Disponível em: <https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html>.

17 OSSF. *Ossf criticality score: Gives criticality score for an open source project*. 2022. Disponível em: <https://github.com/ossf/criticality_score>.

18 OSSF. *OSSF/scorecard: Security scorecards - security health metrics for open source*. 2022. Disponível em: <https://github.com/ossf/scorecard>.

19 SECURE open source rewards. 2022. Disponível em: <https://sos.dev/>.

20 BUSH, M.; MASHATAN, A. From zero to one hundred: Demystifying zero trust and its implications on enterprise people, process, and technology. *Queue*, ACM New York, NY, USA, v. 20, n. 4, p. 80–106, 2022.

21 OLALERE, M.; ABDULLAH, M. T.; MAHMOD, R.; ABDULLAH, A. A review of bring your own device on security issues. *SAGE Open*, v. 5, n. 2, p. 2158244015580372, 2015. Disponível em: <https://doi.org/10.1177/2158244015580372>.

22 MEHRAJ, S.; BANDAY, M. T. Establishing a zero trust strategy in cloud computing environment. In: *2020 International Conference on Computer Communication and Informatics (ICCCI)*. [S.l.: s.n.], 2020. p. 1–6.

23 INITIATIVE, J. T. F. T. *SP 800-207. Zero Trust Architecture*. Gaithersburg, MD, USA, 2020.

24 MARSH, S. P. *Formalising Trust as a Computational Concept*. Tese (Doutorado) — Universidade de Stirling, 1994.

25 DAVIS, M. S. J. *Back to the future: What the jericho forum taught us about modern security*. Microsoft Security Blog, 2020. Disponível em: <https://www.microsoft.com/en-us/security/blog/2020/10/28/back-to-the-future-what-the-jericho-forum-taught-us-about-modern-security/>.

26 ZERO trust working group. Cloud Security Alliance (CSA), 2022. Disponível em: <https://cloudsecurityalliance.org/research/working-groups/zero-trust/>.

27 AMERICA under cyber siege: preventing and responding to ransomware attacks. U.S. Department of Homeland Security, 2021. Disponível em: <https://www.judiciary.senate.gov/imo/media/doc/Goldstein-Statement.pdf>.

28 SHEIKH, N.; PAWAR, M.; LAWRENCE, V. Zero trust using network micro segmentation. In: *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. [S.l.: s.n.], 2021. p. 1–6.

29 KAK, S. *Zero Trust Evolution & Transforming Enterprise Security*. Tese (Doutorado) — CALIFORNIA STATE UNIVERSITY SAN MARCOS, 2022.

30 SUCIU, G.; ISTRATE, C.-I.; VULPE, A.; SACHIAN, M.-A.; VOCHIN, M.; FARAO, A.; XENAKIS, C. Attribute-based access control for secure and resilient smart grids. In: *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*. [S.l.: s.n.], 2019. p. 67–73.

31 COLLIER, Z. A.; SARKIS, J. The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, Taylor & Francis, p. 1–16, 2021. Disponível em: <https://doi.org/10.1080/00207543.2021.1884311>.

32 GROUP), J. B. N. A. S. N. N. B. B. C. G. K. W. B. C. G. A. H. B. C. G. M. F. B. C. *Cyber Supply Chain Risk Management Practices for Systems and Organizations*. Gaithersburg, MD, USA, 2022.

33 DIVISION, C. *Zero Trust Maturity Model*. 245, Murray Lane, Washington, D.C. 20528-0380, 2021.

34 GHADGE, D. A.; WEIB, M.; CALDWELL, N.; WILDING, R. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management*, p. 1–36, 07 2019.

35 YEBOAH-OFORI, A.; ISLAM, S. Cyber security threat modeling for supply chain organizational environments. *Future Internet*, Multidisciplinary Digital Publishing Institute, v. 11, n. 3, p. 63, 2019.

36 SUPPLY CHAIN COMPROMISE: Compromise software supply chain. 2022. Acessado em 09/09/2022. Disponível em: <https://attack.mitre.org/techniques/T1195/002/>.

37 WU, Q.; LU, K. On the feasibility of stealthily introducing vulnerabilities in open-source software via hypocrite commits. In: *Proc. Oakland*. [S.l.: s.n.], 2021.

38 TOPPING, C.; MICHALEC, O.; RASHID, A. *Contrasting global approaches for identifying and managing cybersecurity risks in supply chains*. arXiv, 2022. Disponível em: <https://arxiv.org/abs/2208.02244>.

39 DECRETO nº 11.200, de 15 de setembro de 2022. Plano Nacional de Segurança de Infraestruturas Críticas. Presidência da República, 2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm>.

40 LEI nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Presidência da República, 1999. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm>.

41 DECRETO nº 8.793, de 29 de junho de 2016. Política Nacional de Inteligência. Presidência da República, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>.

42 SUPPLY chain cyber security - National Cyber Security Centre. National Cyber Security Centre, 2022. Disponível em: <https://www.ncsc.gov.uk/files/Assess-supply-chain-cyber-security.pdf>.

43 EXECUTIVE OFFICE OF THE PRESIDENT. EXECUTIVE OFFICE OF THE PRESIDENT, 2022. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>.

44 EXECUTIVE order 14028, improving the nation's cybersecurity. 2022. Disponível em: <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>.

45 SECURE software development framework (ssdf). NIST, 2022. Disponível em: <https://csrc.nist.gov/Projects/ssdf>.

46 SOFTWARE Supply Chain Security Guidance under executive order (eo) 14028. NIST, 2022. Disponível em: <https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf>.

47 THE Minimum Elements For a Software Bill of Materials (SBOM). 2022. Disponível em: <https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf>.

48 RESUMOS digitais (hashes) das eleições 2022 – 1º e 2º turnos. 2022. Disponível em: <https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/hash/resumos-digitais-hashes-das-eleicoes-2022-1o-e-2o-turnos>.

49 INTRODUCING SLSA, an end-to-end framework for Supply Chain Integrity. 2021. Acessado em 09/09/2022. Disponível em: <https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html>.

50 SECURITY Levels. 2022. Disponível em: <https://slsa.dev/spec/v0.1/levels>.

51 TOTO: Specifications. 2022. Acessado em 09/09/2022. Disponível em: <https://in-toto.io/specs/>.

52 SUPPLY chain threats. 2022. Disponível em: <https://slsa.dev/spec/v0.1/#supply-chain-threats>.

53 MICROSOFT. *Supply Chain Integrity Model (SCIM)*. Microsoft, 2021. Disponível em: <https://github.com/microsoft/scim>.

54 IETF-SCITT. *Supply Chain Integrity, Transparency and Trust (SCITT)*. IETF, 2022. Disponível em: <https://scitt.io/>.

55 OWASP. *WWW-project-top-10-ci-cd-security-risks/index.md at main · OWASP/WWW-project-top-10-ci-cd-security-risks*. 2022. Disponível em: <https://github.com/OWASP/www-project-top-10-ci-cd-security-risks/blob/main/index.md>.

56 BEYER, B.; JONES, C.; PETOFF, J.; MURPHY, N. *Site Reliability Engineering: How Google Runs Production Systems*. O'Reilly Media, Incorporated, 2016. ISBN 9781491929124. Disponível em: <https://books.google.com.br/books?id=81UrjwEACAAJ>.

57 CIS Software Supply Chain Security Guide. Center for Internet Security (CIS), 2022. Disponível em: <https://www.cisecurity.org/insights/white-papers/cis-software-supply-chain-security-guide>.

58 AQUASECURITY. *Aquasecurity/chain-bench: An open-source tool for Auditing Your Software Supply Chain Stack for security compliance based on a new CIS Software Supply Chain Benchmark.* 2022. Disponível em: <https://github.com/aquasecurity/chain-bench>.

59 CNCF. *Software Supply Chain Best Practices*. 2022. Disponível em: <https://github.com/cncf/tag-security/tree/main/supply-chain-security>.

60 SIGSTORE. 2022. Disponível em: <https://docs.sigstore.dev/>.

61 RADACK, S. M. et al. Minimum security requirements for federal information and information systems: Federal information processing standard (fips) 200 approved by the secretary of commerce. 2006.

62 BRASIL. Lei nº 13.709, de 14 de agosto de 2018.. lei geral de proteção de dados pessoais (lgpd). *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

63 GENERAL Data Protection Regulation (GDPR). European Union, 2022. Disponível em: <https://gdpr-info.eu/>.

64 CALIFORNIA Consumer Privacy Act (ccpa). State of California - Department of Justice - Office of the Attorney General, 2022. Disponível em: <https://oag.ca.gov/privacy/ccpa>.

65 FORCE, J. T. *NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations — csrc.nist.gov*. 2022. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>. [Accessed 14-Nov-2022].

66 MOORE NICHOLAS ADMAN, K. B. G. *Zero Trust Guidance Center*. Microsoft, 2021. Disponível em: <https://docs.microsoft.com/en-us/security/zero-trust/>.

67 KOSKINEN, A. *DevSecOps : building security into the core of DevOps*. Dissertação (Mestrado) — University of Jyväskylä, http://urn.fi/URN:NBN:fi:jyu-202001171290, 2020.

68 SILVA, A. de Melo e; GONDIM, J. J. C.; ALBUQUERQUE, R. de O.; GARCÍA-VILLALBA, L. J. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet*, v. 12, n. 6, p. 108, 2020. Disponível em: <https://doi.org/10.3390/fi12060108>.

69 KEMPER, S. *Reinventing the Wheel: A Story of Genius, Innovation, and Grand Ambition*. HarperCollins, 2005. ISBN 9780060761387. Disponível em: <https://books.google.com.br/books?id=Lh9aRqDuczUC>.

70 SOFTWARE gratuito e Responsabilidade Jurídica. 2022. Disponível em: <https://www.sedep.com.br/artigos/software-gratuito-e-responsabilidade-juridica/>.

71 CVSS. 2022. Acessado em 09/09/2022. Disponível em: <https://www.first.org/cvss/>.

72 APT29. 2022. Disponível em: <https://attack.mitre.org/groups/G0016/>.

73 RUSSIAN svr targets u.s. and allied networks - u.s. department of defense. Cybersecurity and Infrastructure Security Agency (CISA), 2021. Disponível em: <https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF>.

74 UK and us call out russia for solarwinds compromise. National Cyber Security Centre (NCSC), 2021. Disponível em: <https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise>.

75 WILLETT, M. Lessons of the solarwinds hack. *Survival*, Taylor & Francis, v. 63, n. 2, p. 7–26, 2021.

76 ORION platform. 2022. Disponível em: <https://www.solarwinds.com/en/orion-platform>.

77 MANDIANT. *Highly evasive attacker leverages Solarwinds Supply Chain to compromise multiple global victims with Sunburst Backdoor*. 2020. Disponível em: <https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor>.

78 TEARDROP. 2022. Disponível em: <https://attack.mitre.org/software/S0560/>.

79 TEAM, M. . D. T. I. *Deep dive into the solorigate second-stage activation: From sunburst to teardrop and raindrop*. 2021. Disponível em: <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>.

80 SIGSTORE. *Sigstore proves that effective supply chain security doesn't have to hurt*. sigstore, 2022. Disponível em: <https://blog.sigstore.dev/sigstore-proves-that-effective-supply-chain-security-doesnt-have-to-hurt-cf33cf9333c8>.

81 PEISERT, S.; SCHNEIER, B.; OKHRAVI, H.; MASSACCI, F.; BENZEL, T.; LANDWEHR, C.; MANNAN, M.; MIRKOVIC, J.; PRAKASH, A.; MICHAEL, J. B. Perspectives on the solarwinds incident. *IEEE Security Privacy*, v. 19, n. 2, p. 7–13, 2021.

82 SETTING the new standard in secure software development: the solarwinds next-generation build system. SolarWinds, 2021. Disponível em: <https://www.solarwinds.com/-/media/solarwinds/swresources/whitepaper/2111_swi_whitepaper_nextgenbuild.ashx?rev=3ae62578973a4ed9a8140d6b61425901>.

83 ENCK, W.; WILLIAMS, L. Top five challenges in software supply chain security: Observations from 30 industry and government organizations. *IEEE Security & Privacy*, IEEE, v. 20, n. 2, p. 96–100, 2022.

84 PERSPECTIVES on Security Volume One: Securing Software Supply Chains. Google, 2022. Disponível em: <https://services.google.com/fh/files/blogs/perspectives_on_security_volume_one_digital.pdf>.

85 UNDERSTANDING the impact of Apache Log4j vulnerability. Google, 2021. Disponível em: <https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html>.

86 CYBER threats in the pipeline: lessons from the federal response to the colonial pipeline ransomware attack. House Homeland Security, 2021. Disponível em: <https://www.congress.gov/event/117th-congress/house-event/LC67088/text?s=1&r=63>.

87 SMITH, S. Out of gas: A deep dive into the colonial pipeline cyberattack. In: *SAGE Business Cases*. [S.l.]: SAGE Publications: SAGE Business Cases Originals, 2022.

88 FBI statement on Network Disruption at colonial pipeline. Federal Bureau of Investigation (FBI), 2021. Disponível em: <https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline>.

89 NOCTURNUS, C. *Cybereason vs. Darkside ransomware*. Cybereason, 2021. Disponível em: <https://www.cybereason.com/blog/research/cybereason-vs-darkside-ransomware>.

90 ZETTER, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown, 2015. ISBN 9780770436193. Disponível em: <https://books.google.com.br/books?id=pCfZCwAAQBAJ>.