Capítulo 1

Controles de Segurança para Conformidade baseados em Ferramentas Livres

Security Controls for Compliance Based on Open-Source Tools

Lucas Alionço Perez, Bernardo Pavloski Tomasi, Yago Yudi Vilela Furuta, Marcos Sfair Sunye e André Grégio

Abstract

Ensuring cybersecurity in real scenarios requires the definition of policies and the deployment of controls. There are several standards and normative instructions available to guide the creation of policies and processes, as well as to put those controls in practice. However, it can be difficult to take the first steps into the effective application of these norms when the organization does not have anything in place yet. In this work, we will present selected normatives related to cybersecurity delve into controls to distinguish those that are theoretical/bureaucratic/management-related from the practical ones in order to present and compare the tools and mechanisms that support a quick start for implementing the program in an organization.

Resumo

Garantir a cibersegurança em cenários reais requer a definição de políticas e a implementação de controles. Existem vários padrões e instruções normativas disponíveis para orientar a criação de políticas e processos, assim como a aplicação prática desses controles. No entanto, pode ser difícil dar os primeiros passos na aplicação efetiva de tais normas quando a organização ainda não possui nada estabelecido. Neste trabalho, apresentaremos normas selecionadas relacionadas à cibersegurança e exploraremos os controles para distinguir aqueles que são teóricos, burocráticos ou gerenciais dos que são práticos, a fim de apresentar possibilidades de ferramentas e mecanismos que apoiam um início rápido na implementação do programa em uma organização.

1.1. Introdução

A constante evolução dos avanços tecnológicos e do uso de sistemas computacionais para a maioria das atividades diárias (trabalho, compras, finanças, relacionamentos) tornam

a privacidade e a segurança da informação objetos frequentemente desafiados por um amplo espectro de ameaças digitais. Diversos atores mal-intencionados (incluindo indivíduos, organizações criminosas e órgãos de inteligência de várias nações) se aproveitam das características dos sistemas conectados à Internet (acesso remoto, anônimo e de amplo alcance de usuários) para explorar vulnerabilidades a fim de realizar ataques que comprometam a integridade, confidencialidade e/ou disponibilidade das informações. Tais riscos exigem que organizações de todos os tamanhos e setores busquem formas de identificar, acompanhar e preencher lacunas de privacidade e segurança da informação [SGD 2024b]. Para tanto, foram criados *frameworks* cujo propósito é administrar e reduzir tais riscos, como o *CIS Controls* [CIS 2024f], o *NIST Cybersecurity Framework* [NIST 2024e] e o *Framework* de Programa de Privacidade e Segurança da Informação (PPSI) [SGD 2024b], servindo de guia para indivíduos e organizações na defesa contra ataques cibernéticos.

Embora os referidos *frameworks* sejam projetados para atender organizações de todos os níveis de maturidade em relação a processos de cibersegurança [NIST 2024e], entidades que possuem procedimentos e políticas de segurança da informação bem estabelecidos percebem uma maior facilidade na adoção de novos controles trazidos pelos *frameworks*. Por outro lado, organizações que não possuem o mesmo nível de maturidade organizacional (como pode ser o caso de pequenos e médios negócios, por exemplo) podem encontrar dificuldades em estabelecer e adotar as políticas necessárias para atendimento dos controles de segurança da informação.

Os *frameworks* de segurança citados são apresentados em um alto nível de abstração e consideram que: (a) cada organização possui riscos comuns e/ou únicos; e (b) cada organização admite níveis variados de tolerância a riscos. Por conta dessas diferenças e necessidades, o modo de implementação dos controles de segurança varia entre uma organização e outra [NIST 2024e]. A adoção dos controles na prática tem o apoio da comunidade de cibersegurança para torná-los implementáveis, utilizáveis, escaláveis e alinhados com os requisitos da indústria ou de governos.

Nesse cenário, constrói-se a situação em que organizações sem maturidade administrativa se veem obrigadas a seguir controles rígidos de segurança e privacidade. Apesar de ser uma tarefa exaustiva, é possível observar que mesmo organizações sem políticas e procedimentos de segurança bem definidos podem dar os passos iniciais em direção à conformidade, utilizando ferramentas de software livre. O objetivo deste documento é prover uma análise preliminar dos controles que podem ser atendidos por este tipo de ferramenta e listá-las, de forma a fomentar a adequação aos controles de segurança.

1.2. Principais *frameworks* de Segurança

Para fins de delimitação do escopo deste trabalho, optou-se por detalhar os *frameworks* de segurança que inspiraram o desenvolvimento do *Framework* do Programa de Privacidade e Segurança da Informação (PPSI), de adoção obrigatória por órgãos e entidades da administração pública federal. Destarte, os *frameworks* que serão apresentados neste estudo são os *CIS Controls*, o *NIST Cybersecurity Framework* e o próprio *Framework* de Programa de Privacidade e Segurança da Informação (PPSI).

1.2.1. *CIS Controls*

O CIS (*Center for Internet Security*) é uma entidade sem fins lucrativos globalmente reconhecida pelas melhores práticas em segurança para sistemas da informação. A instituição lidera uma comunidade global de profissionais para promover uma evolução contínua dos padrões de segurança e fornecer produtos e serviços contra ameaças emergentes.

Os *CIS Controls* refletem o conhecimento combinado de especialistas de todas as partes do ecossistema de cibersegurança (indústria, governos e indivíduos), de todas as áreas de atuação (times de resposta a incidentes, analistas de ameaças, pesquisadores de vulnerabilidades, desenvolvedores de ferramentas, usuários, auditores) e em muitos setores das sociedade (governamental, financeiro, transporte, academia, consultoria). Os controles em si são desenvolvidos pela obtenção do consenso entre os especialistas sobre as melhores práticas em segurança. De modo geral, trata-se de aproveitar a experiência de uma comunidade de indivíduos e empresas para realmente fazer melhorias na segurança por meio do compartilhamento de ideias, ferramentas, lições e ações coletivas. Os *CIS Controls* são divididos nos 18 controles a seguir:

1. Inventário e controle de ativos corporativos;
2. Inventário e controle de ativos de software;
3. Proteção de dados;
4. Configuração segura de ativos corporativos e software;
5. Gestão de contas;
6. Gestão de controle de acesso;
7. Gestão contínua de vulnerabilidades;
8. Gestão de registros de auditoria;
9. Proteções de e-mail e navegador Web;
10. Defesas contra *malware*;
11. Recuperação de dados;
12. Gestão da infraestrutura de rede;
13. Monitoramento defesa da rede;
14. Conscientização sobre segurança e treinamento de competências;
15. Gestão de provedor de segurança;
16. Segurança de aplicações;
17. Gestão de resposta a incidentes;
18. Testes de invasão.

Para cada controle é apresentada uma visão geral e explicação sobre a sua criticidade, bem como uma descrição de procedimentos e ferramentas que favorecem a implementação e automação do controle. As medidas de segurança em si são exibidas em uma lista de ações específicas que devem ser realizadas para cumprimento do controle.

Há um total de 153 medidas de segurança distribuídas entre os 18 controles. Embora seja um grande número, nem todas as organizações precisam implementar todos os

controles e medidas de segurança. Os *CIS Controls* apresentam uma forma de priorização das medidas de segurança por grupos de implementação, divididos em três níveis, denominados Grupos de Implementação 1, 2 e 3 [CIS 2024c]. Todas as organizações devem buscar atender aos controles indicados no Grupo de Implementação 1, definido como "ciber higiene". Os grupos subsequentes expandem o Grupo 1. Os Grupos de Implementação são descritos da seguinte forma:

- **Grupo de Implementação 1 (IG1)**: geralmente representa organizações de pequeno e médio porte com recursos limitados de tecnologia da informação e cibersegurança. A sensibilidade dos dados com os quais essas entidades trabalham é baixa, normalmente relacionada a privacidade de empregados e informações financeiras. Os controles e medidas de segurança indicados para este grupo são considerados essenciais, representando o que toda organização deveria aplicar para se proteger dos ataques mais comuns. Das 153 medidas de segurança dos *CIS Controls*, 56 são recomendados para este grupo.

- **Grupo de Implementação 2 (IG2)**: este grupo representa organizações que dispõem de uma equipe responsável por administrar e proteger a sua infraestrutura de TI, além de comportar múltiplos departamentos com diferentes perfis de risco. Organizações que se enquadram nesta categoria podem estar sujeitas à conformidade regulatória e usualmente processam dados sensíveis de clientes ou informações confidenciais para o negócio. Uma brecha de segurança pode causar a perda da confiança no serviço por parte de clientes. Para este grupo, há 74 novas medidas de segurança (que se somam às 56 recomendadas para o IG1).

- **Grupo de Implementação 3 (IG3)**: este grupo engloba entidades maduras, que empregam especialistas de várias áreas de cibersegurança. Os ativos e dados dessas organizações contêm informações sensíveis e/ou estão sujeitos a supervisão regulatória e de conformidade. As atividades desenvolvidas devem sempre atender aos princípios da disponibilidade, integridade e confidencialidade. Falhas de segurança para entidades deste grupo podem resultar em dano significativo ao bem público [CIS 2024d]. As 23 novas medidas de segurança recomendadas para este grupo se somam às 56 do IG1 e às 74 do IG2, totalizando as 153 medidas dos *CIS Controls*. Um exemplo de controle é mostrado na Tabela 1.1.

Os *CIS Benchmarks*, uma documentação complementar do *CIS Controls*, trazem um conjunto de recomendações de configurações para mais de 25 famílias de produtos comumente usados na indústria, incluindo serviços em nuvem, contêineres, bancos de dados, aplicativos *desktop*, servidores, dispositivos móveis, dispositivos de rede e sistemas operacionais [CIS 2024b]. Essas recomendações são desenvolvidas a partir do consenso de especialistas em cibersegurança e representam o esforço da comunidade em proteger sistemas de forma confiável e globalmente. Parte das medidas de segurança recomendadas pelos *CIS Controls* podem ser implementadas a partir da aplicação das configurações seguras indicadas nos *CIS Benchmarks*.

Além disso, os *CIS Controls* podem ser mapeados para outros *frameworks* de cibersegurança, como *NIST Cybersecurity Framework*, *MITRE Enterprise ATT&CK*, SOC

Tabela 1.1. Controle 16.13 do *CIS Controls*, para fins de exemplo.

Controle	16 - Segurança de aplicações
Medida de Segurança	16.13
Título	Realizar teste de invasão de aplicação
Descrição	Realize teste de invasão das aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de lógica de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente uma aplicação como um usuário autenticado e não autenticado.
Tipo de Ativo	Aplicações
Função de Segurança	Proteger
Grupos de Implementação	IG3

2 (*System and Organization Controls 2*), etc [CIS 2024e]. Essa integração possibilita que múltiplos controles de diferentes fontes sejam atendidos simultaneamente [CIS 2024g]. Nota-se que os *CIS Controls* corroboram a proposta deste trabalho: fornecer um ponto de partida para organizações que não possuem políticas ou procedimentos bem definidos, de baixo e médio porte, cuja priorização de medidas de segurança por grupos de implementação e a aplicação dos guias práticos dos *CIS Benchmarks* contribuem significativamente para um início rápido e prático de um programa de segurança.

1.2.2. *NIST Cybersecurity Framework*

O NIST (*National Institute of Standards and Technology*) foi fundado em 1901 e pertence ao Departamento de Comércio dos Estados Unidos [NIST 2024a]. O Instituto possui programas científicos nas mais diversas áreas do conhecimento, incluindo comunicações, biociência, clima, química, infraestrutura, saúde, dentre outros [NIST 2024g]. Destacam-se as pesquisas do NIST em cibersegurança e tecnologia da informação, contexto em que o *NIST Cybersecurity Framework* (CSF) foi desenvolvido [NIST 2024b].

Atualmente em sua versão 2.0, o *NIST Cybersecurity Framework* possui propósito semelhante ao do *CIS Controls*: fornecer orientação para a indústria, órgãos governamentais e outras organizações para gerenciar riscos de segurança cibernética. É destinado a todos os tipos de organizações, independentemente de tamanho, setor ou maturidade e auxilia no processo de compreender, avaliar, priorizar e comunicar melhor os esforços de segurança cibernética. O público principal do *NIST Cybersecurity Framework* é composto por profissionais responsáveis por desenvolver e liderar programas de segurança cibernética em organizações. Entretanto, o *framework* também pode ser utilizado por outras pessoas envolvidas no gerenciamento de riscos, como executivos, conselhos de administração, advogados, especialistas em recursos humanos e auditores [NIST 2024e].

Da mesma forma que ocorre com os *CIS Controls*, o *NIST Cybersecurity Framework* não prescreve como os resultados devem ser alcançados: em vez disso, ele descreve os resultados desejados, associando recursos *on-line* e orientações adicionais que podem ser usados para alcançar tais resultados [NIST 2024e]. A descrição dos resultados

almejados é neutra em termos de setor, país e tecnologia, o que viabiliza a flexibilidade necessária para a implementação dos controles.

O *CSF Core* (um apêndice complementar ao documento principal do *NIST Cybersecurity Framework*) define o conjunto de controles de segurança e resultados esperados pelas organizações. Ele é estruturado em funções, categorias e subcategorias. As funções representam os objetivos de segurança em seu nível mais abrangente, enquanto as categorias e subcategorias especificam as ações técnicas e de gerenciamento necessárias para atingir esses objetivos. Cada função, categoria e subcategoria abrange uma série de atividades que auxiliam nas etapas de compreensão, avaliação, priorização e comunicação, fundamentais para a implementação eficaz da segurança cibernética [NIST 2024d]. As seis funções do *NIST CSF Core* são:

- **GOVERNAR (*GOVERN* - GV)**: esta função determina que a estratégia, as expectativas e a política de gerenciamento de riscos de segurança cibernética da organização sejam estabelecidas, comunicadas e monitoradas. A função de Governar oferece insumo para informar o que a organização pode fazer para atingir e priorizar os resultados das outras cinco funções. Envolve atividades de estratégia de segurança cibernética, elaboração de políticas e gerenciamento de riscos.
- **IDENTIFICAR (*IDENTIFY* - ID)**: esta função determina que os riscos atuais de segurança cibernética da organização sejam compreendidos. Inclui atividades de compreensão sobre os ativos da organização (dados, hardware, software, sistemas, instalações, serviços), de fornecedores e de riscos relacionados à segurança cibernética, bem como atividades de identificação de oportunidades de melhoria para as políticas, planos, processos e práticas da organização.
- **PROTEGER (*PROTECT* - PR)**: esta função determina que sejam usadas proteções para gerenciar os riscos de segurança cibernética da organização, com o objetivo de proteger os ativos identificados. Inclui atividades de gerenciamento de identidades e controle de acesso, conscientização e treinamento, segurança de dados e de sistemas.
- **DETECTAR (*DETECT* - DE)**: esta função determina que possíveis ataques e comprometimentos de segurança devem ser encontrados e analisados. A detecção oportuna de anomalias, indicadores de comprometimento e outros eventos adversos oferece suporte para as atividades de resposta e recuperação de incidentes.
- **RESPONDER (*RESPOND* - RS)**: esta função determina que ações relacionadas a um incidente de segurança detectado devem ser tomadas. Esta função apoia a capacidade de conter os efeitos de um incidente e envolve atividades de gerenciamento, análise, atenuação e comunicação de incidentes.
- **RECUPERAR (*RECOVER* - RC)**: esta função determina que os ativos e as operações afetadas por um incidente de segurança sejam restaurados, garantindo a operação normal da companhia.

Quando analisadas em conjunto, as funções do CSF fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento de risco de cibersegurança de uma

organização [SGD 2024b]. Por essa razão, o NIST apoia a representação das funções do CSF como uma roda, onde todas as funções estão relacionadas entre si. As ações da função Identificar apoiarão as ações da função Proteger, enquanto as atividades da função Detectar fornecem a base para as ações de Responder e Recuperar, por exemplo. A função de Governar se situa no centro da roda pois guia a forma de implementação das outras funções [NIST 2024e].

As seis funções do CSF abrigam 22 categorias e 107 subcategorias de resultados desejados, que partem de uma descrição de alto nível (funções) e se detalham em categorias e subcategorias [NIST 2024e]. Um exemplo de resultado a ser alcançado em uma organização, de acordo com o *NIST CSF Core*, é o resultado ID.AM-02, apresentado na tabela 1.2.

Tabela 1.2. Controle ID.AM-02 do *NIST CSF Core*, para fins de exemplo.

Função	Identificar (ID): os riscos atuais de segurança cibernética da organização são compreendidos.
Categoria	Gerenciamento de ativos (ID.AM): os ativos (por exemplo, dados, hardware, software, sistemas, instalações, serviços, pessoas) que permitem que a organização atinja seus objetivos comerciais são identificados e gerenciados de acordo com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.
Subcategoria	ID.AM-02: os inventários de software, serviços e sistemas gerenciados pela organização são mantidos.

O *NIST Cybersecurity Framework* também se adequa à proposta deste estudo ao oferecer um *Quick Start Guide* para pequenos negócios dentre seus materiais complementares, destinado às organizações com nenhum ou poucos planos para cibersegurança. O guia elenca alguns resultados que podem ser priorizados por essas organizações, facilitando o início rápido na implementação de controles de segurança [NIST 2024d]. Entretanto, não existe o apoio prático como visto nos *CIS Benchmarks*. O NIST oferece uma tabela com exemplos de implementação de medidas que alcançam os resultados desejados, mas todos são descritos em alto nível [NIST 2024c]. Tal como os *CIS Controls*, é possível obter um mapeamento das funções do *NIST CSF Core* para outros *frameworks* [NIST 2024f].

1.2.3. *Framework* de Programa de Privacidade e Segurança da Informação (PPSI)

O Programa de Privacidade e Segurança da Informação (PPSI) foi instituído pelo Ministério da Gestão e da Inovação em Serviços Públicos e sua Secretaria de Governo Digital por meio da Portaria nº 852, de 28 de março de 2023 [SGD 2023b]. Trata-se de um conjunto de projetos e processos distribuídos nas áreas temáticas de governança, maturidade, pessoas, metodologia e tecnologia que têm como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito da administração pública federal direta, autárquica e fundacional.

O artigo 7º da portaria também institui o *Framework* de Privacidade e Segurança da Informação, composto por um conjunto de controles, metodologias e ferramentas de apoio. As bases do *framework* são a Lei Geral de Proteção de Dados Pessoais - LGPD

(Lei nº 13.709 de 14 de agosto de 2018), a Política Nacional de Segurança da Informação - PNSI, os próprios *CIS Controls* e o *Framework* de Privacidade do NIST, normas ISO/IEC e ABNT, normativos emitidos pela Autoridade Nacional de Proteção de Dados - ANPD e pelo Gabinete de Segurança Institucional - GSI, dentre outros [SGD 2023a].

A estratégia adotada pelo *Framework* do PPSI de se apresentar como uma combinação de algumas das referências mais abrangentes viabiliza a complementação e supressão de eventuais lacunas que cada documento base pode trazer. Dessa forma, o *Framework* do PPSI consegue atender a pluralidade de serviços e de tratamento de dados pessoais pelo Poder Público, que possui diversos órgãos com políticas públicas próprias e atribuições institucionais específicas [SGD 2024b].

O *Framework* do PPSI também fornece mecanismos de medição dos índices de maturidade em privacidade e segurança da informação (índices *iSeg* e *iPriv*) do órgão implementador, que podem, por sua vez, subsidiar a implementação e o monitoramento dos controles de privacidade e segurança [SGD 2024b].

O *Framework* do PPSI apresenta um total de 310 medidas de segurança e privacidade, descritas em forma de perguntas, divididas em 31 controles e priorizadas de acordo com grupos de implementação. O PPSI também traz um modelo de avaliação de criticidade de sistemas adaptado do modelo utilizado pelo Tribunal de Contas da União (TCU), a fim de determinar o nível de criticidade e a qual grupo de implementação um órgão implementador do PPSI se enquadra [SGD 2024b]. Os controles do PPSI são divididos da seguinte forma:

- 7 medidas de Controle 0 (Controle de Estruturação Básica em Gestão em Privacidade e Segurança da Informação), aplicáveis a todos os órgãos;
- 56 medidas de cibersegurança e 97 medidas de privacidade para o Grupo 1. Essas medidas são de higiene cibernética e obrigações dispostas na LGPD, também aplicáveis a todos os órgãos;
- 74 medidas de cibersegurança e 32 medidas de privacidade para o Grupo 2. Essas medidas são aplicáveis para órgãos de média criticidade.
- 23 medidas de cibersegurança e 16 medidas de privacidade para o Grupo 3. Essas medidas são aplicáveis para órgãos de alta criticidade.

Um exemplo de controle de cibersegurança trazido pelo PPSI é o controle 6.4, descrito na tabela 1.3.

O *framework* do PPSI é acompanhado de um conjunto de materiais complementares associados aos controles, constituído principalmente por modelos de políticas (como modelos de política de gestão de *logs* de auditoria e de backup) e guias de propósito geral (como um guia de resposta a incidentes de segurança e um guia sobre sobre boas práticas dentro da LGPD). Estes materiais podem ser adotados integralmente ou adaptados ao contexto e necessidade de cada organização [SGD 2024a]. Ressalta-se que apenas a adoção de uma política ou de um guia não cumpre, por si só, o controle de segurança, mas fornece forte embasamento para outras ações.

Tabela 1.3. Controle 6.4 do PPSI, para fins de exemplo.

ID	6.4
ID CIS	6.3
FUNÇÃO NIST CSF	Proteger
MEDIDA	O órgão exige MFA (*Multi-Factor Authentication*) para aplicações expostas externamente?
DESCRIÇÃO DA MEDIDA	Exigir que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA. Impor o MFA por meio de um serviço de diretório ou provedor de SSO (*Single Sign-On*) é uma implementação satisfatória desta medida de segurança.
REFERÊNCIAS LGPD	Art 6º, inciso VII, Art. 46, Art. 47, Art. 49, Art. 50.
REFERÊNCIAS GSI	IN nº 5/2021 NC 01/IN02/NSC/GSIPR e seus anexos (Anexo A e Anexo B).
GRUPOS DE IMPLEMENTAÇÃO	1, 2, 3

Percebe-se que o PPSI se preocupa em expandir os conceitos trazidos por *frameworks* reconhecidos, adaptá-los ao contexto da Administração Pública, aprimorá-los no que for possível e expandi-los nas questões de privacidade, tornando-se um *framework* completo e fundamentado. As correlações entre os controles e as referências legais e administrativas agregam qualidade ao *framework* desenvolvido pela Secretaria de Governo Digital.

1.3. Controles e Medidas de Segurança do *Framework* do PPSI

Atender aos controles de segurança previstos no *CIS Controls*, *NIST CSF Core* e PPSI demanda a utilização de recursos de diversas naturezas. Certos controles podem ser satisfeitos a partir da adoção de políticas dentro da organização, enquanto outros demandam a utilização de ferramentas computacionais específicas para garantir que os padrões de segurança sejam atendidos. Classificar os controles para diferenciar aqueles que são teóricos, burocráticos ou gerenciais daqueles que são práticos e que podem ser prontamente atendidos é necessário para que organizações sem planos em cibersegurança consigam dar seus primeiros passos em direção à conformidade. Ao mesmo tempo, também é preciso se atentar aos controles priorizados de acordo Grupos de Implementação, focando nas ações de higiene cibernética do Grupo 1, descrito na seção 1.2.1.

É importante ressaltar que os controles e as medidas de segurança são sensíveis ao contexto em que se busca implementá-los. Por exemplo, uma medida que indica a necessidade de controle de acesso a dados pode fazer referência a dados no nível do sistema operacional, a dados dentro de um serviço web ou a dados disponíveis em um servidor na nuvem. Em outras palavras, uma mesma medida pode ser implementada de diferentes formas, de acordo o com contexto trabalhado. É o que ocorre quando uma mesma medida é abordada de diferentes formas dentro dos documentos dos *CIS Benchmarks*, que tratam de segurança em níveis distintos (sistemas operacionais, servidores em nuvem,

dispositivos móveis etc). Detalhes sobre cada controle de segurança e suas medidas serão abordados a seguir.

1.3.1. Controle 1: Inventário e Controle de Ativos Institucionais

O primeiro controle de segurança tratado pelo *framework* do PPSI faz referência a ações de inventário e controle de ativos institucionais. Inventariar, rastrear e corrigir os ativos conectados à rede facilita a identificação daqueles que demandam maiores recursos em monitoramento e proteção, ao mesmo tempo em que os ativos não autorizados podem ser selecionados para futura remoção ou tratamento[SGD 2024b].

No contexto deste controle, consideram-se ativos institucionais os dispositivos de usuário final (como computadores e dispositivos móveis), dispositivos de rede (como *switches*), dispositivos não computacionais, dispositivos IoT (Internet das Coisas) e servidores, tanto os conectados à infraestrutura quanto virtuais, remotos e aqueles em ambiente de nuvem.

Mapear os ativos institucionais é uma atividade crucial para garantia da segurança da informação, dado que não é possível proteger aquilo que não é mapeado ou que não se tem conhecimento sobre sua existência [SGD 2024b]. O conceito de *shadow IT* (ou TI invisível) trata de quaisquer dispositivos não autorizados em uso dentro das organizações. Podem ser dispositivos particulares que contenham informações sensíveis do órgão ou repositórios em nuvem não autorizados [IBM 2024]. O problema surge quando esses dispositivos não protegidos são comprometidos, prejudicando as atividades da organização e/ou causando prejuízos.

Este controle de segurança é composto por 5 medidas:

Medida 1.1 - O órgão estabelece e mantém um inventário detalhado de ativos institucionais?

Medida 1.2 - O órgão usa o *Dynamic Host Configuration Protocol* (DHCP) para Atualizar o Inventários de Ativos?

Medida 1.3 - O órgão usa uma ferramenta de descoberta ativa?

Medida 1.4 - O órgão usa ferramenta de Descoberta Passiva?

Medida 1.5 - O órgão endereça ativos não autorizados?

De forma complementar, o *framework* do PPSI também traz um Modelo de Política de Gestão de Ativos que pode auxiliar as organizações a implementar as medidas deste controle de segurança.

Todas as 5 medidas deste controle de segurança admitem uma implementação rápida pelo uso de ferramentas de software livre, indicadas na próxima seção.

1.3.2. Controle 2: Inventário e Controle de Ativos de Software

O segundo controle de segurança abordado pelo PPSI também trabalha questões de inventário e controle de ativos, mas desta vez no âmbito de software. Este controle se preocupa em identificar quais programas se encontram em execução na rede e impedir a execução ou instalação de software não autorizado [SGD 2024b].

Atacantes constantemente fazem varreduras na infraestrutura do alvo em busca de softwares desatualizados ou vulneráveis para explorar vulnerabilidades. Com um inventário de software completo, a organização pode determinar quais as versões dos softwares estão em execução e descobrir aplicações executadas sem permissão [SGD 2024b].

Este controle de segurança é composto por 7 medidas:

Medida 2.1 - O órgão estabelece e mantém um inventário de software?

Medida 2.2 - O órgão assegura que o software autorizado seja atualmente suportado?

Medida 2.3 - O órgão possui lista de permissões de software atualizado?

Medida 2.4 - O órgão possui lista de permissões de bibliotecas autorizadas?

Medida 2.5 - O órgão possui lista de permissões de *Scripts* autorizados?

Medida 2.6 - O órgão utiliza ferramentas automatizadas de inventário de software?

Medida 2.7 - O órgão endereça o software não autorizado?

O mesmo Modelo de Política de Gestão de Ativos trazido pelo PPSI para auxiliar na implementação de medidas do Controle 1 também possui disposições válidas para o Controle 2. Além disso, algumas formas de implementação das medidas deste controle podem ser encontradas nos *CIS Benchmarks* (como, por exemplo, as medidas 2.2, 2.6 e 2.7, que são abordadas no documento *CIS NGINX Benchmark* v2.1.0 [CIS 2024a]).

Das 7 medidas de segurança deste controle, 4 delas favorecem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.3. Controle 3: Proteção de Dados

O terceiro controle abordado pelo PPSI aborda processos e ferramentas para identificar, classificar, manusear, reter e descartar dados. Neste contexto, o PPSI não se preocupa apenas com dados que estão dentro da estrutura das instituições, mas também com aqueles que estão na nuvem, em dispositivos portáteis do usuário final, compartilhados com terceiros ou serviços *on-line* [SGD 2024b].

A proteção de dados é assunto de destaque em todo o cenário global. Gerenciar os dados de maneira adequada durante todo seu ciclo de vida se tornou uma necessidade e vai além das questões de criptografia [SGD 2024b]. Além disso, regulamentações ressaltam também como os dados pessoais devem ser tratados, a exemplo da LGPD no Brasil e GDPR (*General Data Protection Regulation*) da União Europeia.

A perda do controle sobre os dados protegidos ou sensíveis causa impactos sérios ao negócio, com prejuízos financeiros e reputacionais. Além disso, o vazamento indevido de dados pode ferir direitos e garantias individuais dos seus titulares.

Este controle é composto por 14 medidas de segurança:

Medida 3.1 - O órgão estabelece e mantém um processo de gestão de dados?

Medida 3.2 - O órgão estabelece e mantém um inventário de dados?

Medida 3.3 - O órgão estabelece e mantém um esquema de classificação de dados?

Medida 3.4 - O órgão documenta os Fluxos de Dados?

Medida 3.5 - O órgão configura listas de controle de acesso a dados?

Medida 3.6 - O órgão aplica retenção de dados?

Medida 3.7 - O órgão descarta dados com segurança?

Medida 3.8 - O órgão criptografa dados em dispositivos de usuário final?

Medida 3.9 - O órgão criptografa dados em mídia removível?

Medida 3.10 - O órgão criptografa dados sensíveis em trânsito?

Medida 3.11 - O órgão criptografa dados sensíveis em repouso?

Medida 3.12 - O órgão segmenta o processo e o armazenamento de dados com base na sensibilidade?

Medida 3.13 - O órgão implanta uma solução de prevenção contra perda de dados?

Medida 3.14 - O órgão registra o acesso a dados sensíveis?

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Elaboração do Processo de Gestão de Dados e o Modelo de Política de Gestão de Registros (*Logs*) de Auditoria, com enfoque na gestão de Dados, no fluxo dos dados e na classificação de dados [SGD 2024b].

Das 14 medidas de segurança deste controle, 10 delas admitem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção, em nível de sistemas operacionais e sistemas distribuídos.

1.3.4. Controle 4: Configuração Segura de Ativos Institucionais e Software

O controle 4 do *framework* do PPSI trata da configuração segura de ativos institucionais (incluindo dispositivos de usuário final, portáteis, dispositivos de rede, IoT e servidores) e de software. Este controle complementa os controles 1 e 2, buscando utilizar configurações seguras para os dispositivos e software utilizados.

O conjunto padrão de configurações normalmente é voltado para facilidade de implantação e uso, enquanto deixa aspectos de segurança em segundo plano. A configuração padrão pode carregar os sistemas com serviços e portas abertas, contas ou senhas padrão e softwares desnecessários pré-instalados que podem ser explorados por um atacante [SGD 2024b]. Além disso, atualizações de segurança precisam ser gerenciadas para garantir que as configurações seguras não se alterem automaticamente.

Este controle é composto por 12 medidas de segurança:

Medida 4.1 - O órgão estabelece e mantém um processo de configuração segura?

Medida 4.2 - O órgão estabelece e mantém um processo de configuração segura para a Infraestrutura de Rede?

Medida 4.3 - O órgão configura o bloqueio automático de sessão nos ativos?

Medida 4.4 - O órgão implementa e gerencia um *firewall* nos servidores?

Medida 4.5 - O órgão implementa e gerencia um *firewall* nos dispositivos de usuário final?

Medida 4.6 - O órgão gerencia com segurança os ativos corporativos e softwares?

Medida 4.7 - O órgão gerencia contas padrão nos ativos corporativos e software?

Medida 4.8 - O órgão desinstala ou desativa serviços desnecessários nos ativos e software?

Medida 4.9 - O órgão configura servidores DNS (*Domain Name System*) confiáveis nos ativos?

Medida 4.10 - O órgão impõe a capacidade de limpeza remota nos dispositivos portáteis do usuário final?

Medida 4.11 - O órgão separa os Espaços de Trabalho nos dispositivos móveis?

Medida 4.12 - O órgão impõe o bloqueio automático de dispositivos nos dispositivos portáteis de usuário final?

Benchmarks do CIS para *Ubuntu 12.04 LTS Server, NGINX* e *Google Chrome* também mencionam formas de implementar uma parte das medidas deste controle e podem ser utilizados de forma complementar [CIS 2024a].

Das 14 medidas de segurança deste controle, 3 delas viabilizam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.5. Controle 5: Gestão de Contas

O Controle 5 foca em processos e ferramentas para atribuir e gerenciar autenticação de credenciais para contas de usuário, contas de administrador, conta de serviço para ativos e softwares institucionais. A gestão de contas é tarefa crítica no contexto de segurança da informação pois, sem ela, atacantes podem buscar acesso não autorizado aos recursos da organização por uso de senhas fracas ou repetidas de outros serviços, contas válidas de usuários inativos, etc. Contas administrativas ou com alto privilégio e contas de serviço são críticas, pois seu uso possibilita que atacantes adicionem novas contas e façam alterações nos ativosda organização [SGD 2024b].

Este controle é composto por 6 medidas:

Medida 5.1 - O órgão estabelece e mantém um inventário de contas?

Medida 5.2 - O órgão estabelece e mantém um inventário de contas de serviço?

Medida 5.3 - O órgão usa senhas exclusivas?

Medida 5.4 - O órgão restringe privilégios de administrador a contas de administrador dedicadas?

Medida 5.5 - O órgão centraliza a gestão de contas?

Medida 5.6 - O órgão desabilita contas inativas?

Assim como ocorre nos controles anteriores, a Secretaria de Governo Digital dis-

ponibiliza um Modelo de Política de Controle de Acesso que pode ser usado de forma complementar, focado em diretrizes para gestão de controle de acesso [SGD 2024b]. Os *benchmarks* do CIS para *Ubuntu 12.04 LTS Server* e *NGINX* [CIS 2024a] também mencionam medidas deste controle.

Todas as 6 medidas deste controle de segurança admitem uma implementação rápida pelo uso de ferramentas de software livre, indicadas na próxima seção.

1.3.6. Controle 6: Gestão de Controle de Acesso

O controle 6 do *framework* do PPSI foca em questões de autorização de acesso a recursos da organização por uso de ferramentas e processos para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios. Este controle busca assegurar que os usuários tenham acesso apenas aos dados ou ativos necessários para execução de suas funções [SGD 2024b], seguindo o princípio do privilégio mínimo.

Este controle é composto por 8 medidas:

Medida 6.1 - O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?

Medida 6.2 - O órgão estabelece Processo de Concessão de Acesso?

Medida 6.3 - O órgão estabelece Processo de Revogação de Acesso?

Medida 6.4 - O órgão exige MFA (*Multi-Factor Authentication*) para aplicações expostas externamente?

Medida 6.5 - O órgão exige MFA para acesso remoto à rede?

Medida 6.6 - O órgão exige MFA para acesso administrativo?

Medida 6.7 - O órgão centraliza o controle de acesso?

Medida 6.8 - O órgão define e mantém o controle de acesso baseado em funções?

O mesmo Modelo de Política de Controle de Acesso tratado no Controle 5 também pode ser aproveitado para este Controle, seguindo a recomendação da Secretaria de Governo Digital. Uma das medidas também é tratada pelo *Benchmark* do CIS para *Ubuntu 12.04 LTS Server*.

Das 8 medidas de segurança deste controle, 3 delas possibilitam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.7. Controle 7: Gestão Contínua de Vulnerabilidades

O sétimo controle do PPSI trata da gestão de vulnerabilidades. O gerenciamento delas envolve o desenvolvimento de um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura, a fim de remediar e minimizar as janelas de oportunidade para atacantes. A inteligência sobre novas vulnerabilidades pode vir de *patches* de segurança, atualizações de software, avisos de segurança, boletins de ameaça e outros [SGD 2024b].

Este controle é composto por 7 medidas de segurança:

Medida 7.1 - O órgão realiza varreduras automatizadas de vulnerabilidades em ativos institucionais internos?

Medida 7.2 - O órgão realiza varreduras automatizadas de vulnerabilidades em ativos institucionais expostos externamente?

Medida 7.3 - O órgão estabelece e mantém um processo de gestão de vulnerabilidades?

Medida 7.4 - O órgão executa a gestão automatizada de *patches* do sistema operacional?

Medida 7.5 - O órgão executa a gestão automatizada de *patches* de aplicações?

Medida 7.6 - O órgão estabelece e mantém um processo de remediação?

Medida 7.7 - O órgão corrige vulnerabilidades detectadas?

Há um Guia de Gerenciamento de Vulnerabilidades e um Modelo de Política de Gerenciamento de vulnerabilidades disponibilizado como material complementar ao *framework* do PPSI, com enfoque na construção de processos de gerenciamento de vulnerabilidades [SGD 2024b]. Os três *benchmarks* do CIS estudados (*Ubuntu 12.04 LTS Server, NGINX* e *Google Chrome*) também abordam medidas deste controle.

Das 8 medidas de segurança deste controle, 2 delas viabilizam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.8. Controle 8: Gestão Registros de Auditoria

O oitavo controle do PPSI trata da coleta, alerta, análise e retenção de *logs* com o objetivo de detectar, compreender ou se recuperar de um ataque. Muitas vezes, registros de *log* são a única evidência de um ataque bem-sucedido contra a organização. A falta ou insuficiência de um processo de análise de *logs* pode possibilitar que um atacante controle um ativo institucional por meses ou anos sem que seja detectado [SGD 2024b].

No contexto deste controle, um *log* de sistema tipicamente fornece registros de eventos que mostram vários dados de processos, como tempo de início e fim, *crashes*, e etc. *Logs* de auditoria tipicamente incluem informações a nível de usuário, como informações sobre quando um login é feito e quando um arquivo é acessado, por exemplo.

Este controle é composto por 12 medidas de segurança:

Medida 8.1 - O órgão estabelece e mantém um processo de gestão de *log* de auditoria?

Medida 8.2 - O órgão garante o armazenamento adequado do registro de auditoria?

Medida 8.3 - O órgão padroniza a sincronização de tempo?

Medida 8.4 - O órgão retém os *logs* de auditoria?

Medida 8.5 - O órgão coleta *logs* de auditoria?

Medida 8.6 - O órgão coleta *logs* de auditoria detalhados?

Medida 8.7 - O órgão coleta *logs* de auditoria de consulta de DNS?

Medida 8.8 - O órgão coleta *logs* de auditoria de requisição de URL?

Medida 8.9 - O órgão coleta *logs* de auditoria de linha de comando?

Medida 8.10 - O órgão centraliza os *logs* de auditoria?

Medida 8.11 - O órgão conduz revisões de *log* de auditoria?

Medida 8.12 - O órgão coleta *logs* do provedor de serviços?

Há um Modelo de Política de Gestão de Registros (*Logs*) de Auditoria disponibilizado como material complementar ao *framework* do PPSI. Além disso, os três *benchmarks* do CIS estudados *(Ubuntu 12.04 LTS Server*, *NGINX* e *Google Chrome*) também abordam medidas deste controle.

Das 12 medidas de segurança deste controle, 4 delas admitem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.9. Controle 10: Defesas contra *Malware*

O décimo controle de segurança do PPSI trata da defesa contra instalação, execução e disseminação de aplicações, códigos ou *scripts* maliciosos em ativos da organização.

Softwares maliciosos estão em constante evolução e adaptação, exigindo que as ferramentas de defesa contra *malware* sejam capazes de operar neste ambiente dinâmico. Ferramentas antivírus deve contar com funcionalidades de automação, atualização rápida, oportuna e integração com outros processos, como de gestão de vulnerabilidades e resposta a incidentes. Esses softwares de defesa devem ser instalados em todos os possíveis pontos de entrada e ativos institucionais, considerando que grande parte dos ataques ocorre por conta de comportamento inseguro dos usuários finais, como cliques em links estranhos e uso de dispositivos USB infectados [SGD 2024b].

Este controle é composto por 7 medidas:

Medida 10.1 - O órgão instala e mantém um software *antimalware*?

Medida 10.2 - O órgão configura atualizações automáticas de assinatura *antimalware*?

Medida 10.3 - O órgão desabilita a execução e produção automática para mídias removíveis?

Medida 10.4 - O órgão habilita funções antiexploração?

Medida 10.5 - O órgão gerencia o software *antimalware* de maneira centralizada?

Medida 10.6 - O órgão configura a varredura *antimalware* automática de mídia removível?

Medida 10.7 - O órgão utiliza software *antimalware* baseado em comportamento?

O documento *CIS Ubuntu 12.04 LTS Server Benchmark v1.1.0* trata de parte das medidas deste controle e pode ser usado como referência na configuração de um sistema operacional, principalmente nas questões sobre execução de mídias removíveis. Além

disso, a SGD disponibiliza um Modelo de Política de Defesas contra *Malware*, que pode ser utilizado de forma complementar [SGD 2024b].

Das 7 medidas de segurança deste controle, 2 delas apoiam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.10. Controle 11: Recuperação de Dados

O controle 11 se atenta à capacidade da organização de recuperar seus dados e os ativos em situações de incidentes para um estado anterior confiável. Nos casos em que um atacante obtém acesso a um ativo da instituição e o torna inseguro, é necessário ter a possibilidade de se valer de *backups* confiáveis para restaurar o dispositivo ou dados para um momento conhecido e seguro.

Nota-se também que um ativo institucional pode ser alvo de um *ransomware*, um tipo de *malware* que criptografa e sequestra os dados de um órgão, exigindo o pagamento de uma quantia para desbloqueio. Embora a utilização de um *backup* confiável possa recuperar o ativo ou os dados, os atacantes ainda podem vender ou divulgar os dados sequestrados.

Este controle é composto por 5 medidas:

Medida 11.1 - O órgão protege os dados de recuperação?

Medida 11.2 - O órgão estabelece e mantém um processo de recuperação de dados?

Medida 11.3 - O órgão executa backups automatizados?

Medida 11.4 - O órgão estabelece e mantém uma instância isolada de dados de recuperação?

Medida 11.5 - O órgão testa os dados de recuperação?

A secretaria de Governo Digital disponibiliza um Modelo de Política de Backup focado na construção das políticas de *backup* e restauração de dados digitais da instituição, que pode ser utilizado como material complementar na implementação das medidas [SGD 2024b].

Das 5 medidas de segurança deste controle, 4 delas apoiam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.11. Controle 12: Gestão de Infraestrutura de Rede

Este controle foca em estabelecer, implementar e gerenciar ativamente os dispositivos de rede para evitar a exploração de serviços e pontos de acesso vulneráveis por atacantes. Uma infraestrutura de rede segura constitui uma defesa essencial contra atacantes e inclui aspectos de arquiteturas seguras, monitoramento de alterações ao longo do tempo e reavaliação regular das configurações atuais.

Além disso, a rede de um órgão pode estar em constante mudança, o que exige a análise regular dos diagramas de arquitetura, configurações, controles de acesso e fluxos de tráfego, tudo a fim de evitar que atacantes se aproveitem de pontos vulneráveis não

identificados. Este controle se relaciona com outros, como de gestão de ativos, proteção contra *malware* e registros de *logs*, por exemplo.

Este controle é composto por 8 medidas:

Medida 12.1 - O órgão elabora e mantém diagramas de arquitetura?

Medida 12.2 - O órgão garante que a infraestrutura de rede está atualizada?

Medida 12.3 - O órgão garante níveis de segurança para a arquitetura de rede?

Medida 12.4 - O órgão gerencia a infraestrutura de rede e segurança?

Medida 12.5 - O órgão centraliza a autenticação, autorização e auditoria de rede (AAA)?

Medida 12.6 - O órgão utiliza protocolos de comunicação e gestão de rede seguros?

Medida 12.7 - O órgão garante que os dispositivos remotos utilizam uma VPN (*Virtual Private Network*) e se conectem em uma infraestrutura AAA segura da organização?

Medida 12.8 - O órgão utiliza e mantém recursos cibernéticos dedicados para todo o trabalho administrativo?

Como mencionado, medidas deste controle podem ser complementadas pelos Modelos de Política de Gestão de Ativos, de Controle de Acesso, de gestão de Registros (*Logs*) de Auditoria e de Defesas contra *Malware*, todos disponibilizados pela SGD.

Das 8 medidas de segurança deste controle, 1 delas viabiliza uma implementação rápida pelo uso de ferramentas de software livre e será abordada na próxima seção.

1.3.12. Controle 13: Monitoramento e Defesa da Rede

O controle 13 se atenta aos processos e ferramentas para monitoramento e defesa da rede do órgão contra ataques em sua infraestrutura. Um monitoramento eficaz das atividades da rede garante que a equipe seja alertada sobre atividades suspeitas e responda prontamente a incidentes de segurança, como quando um *malware* é descoberto, credenciais são roubadas ou quando dados sensíveis são comprometidos [SGD 2024b].

Este controle é composto por 11 medidas:

Medida 13.1 - O órgão realiza filtragem de tráfego entre os segmentos de rede?

Medida 13.2 - O órgão aplica o gerenciamento de controle de acesso em ativos remotos?

Medida 13.3 - O órgão implanta soluções de prevenção de intrusão baseada em *host*?

Medida 13.4 - O órgão implanta soluções para prevenção de intrusão de rede?

Medida 13.5 - O órgão implanta controle de acesso a nível de porta?

Medida 13.6 - O órgão realiza a filtragem de camada de aplicação?

Medida 13.7 - O órgão centraliza alertas de eventos de segurança?

Medida 13.8 - O órgão implanta soluções de detecção e intrusão baseada em *host*?

Medida 13.9 - O órgão realiza filtragem de tráfego entre os segmentos de rede?

Medida 13.10 - O órgão coleta *logs* de fluxo e tráfego de rede?

Medida 13.11 - O órgão ajusta os limites de alertas de eventos de segurança?

Das 11 medidas de segurança deste controle, 3 delas admitem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.13. Controle 16: Segurança de Aplicações

Partindo para o nível de aplicação, o controle 16 se atenta à segurança ao longo do ciclo de vida dos softwares desenvolvidos e adquiridos internamente, a fim de detectar e corrigir falhas de segurança.

Além de se aproveitar das credenciais adquiridas por técnicas de engenharia social, um atacante podem explorar vulnerabilidades que encontrar nas aplicações desenvolvidas pelo próprio órgão para gerenciar seus dados e demais recursos. O processo de desenvolvimento de software é complexo, diverso, dinâmico e aplicado em várias plataformas como web, móvel e nuvem. Essa amplitude de espaços que as aplicações podem ocupar também representa uma vasta superfície de ataque para indivíduos mal intencionados. Vulnerabilidades podem existir em um projeto ou infraestrutura insegura, erros de codificação, autenticação fraca e falha nos testes de software [SGD 2024b].

No contexto em que grande parte dos softwares utilizados são providos por terceiros, a organização precisa conhecer os riscos envolvidos na utilização desses programas.

Este controle é composto por 14 medidas:

Medida 16.1 - O órgão estabelece e mantém um processo de desenvolvimento de aplicações?

Medida 16.2 - O órgão estabelece e mantém um processo para aceitar e endereçar vulnerabilidades de software?

Medida 16.3 - O órgão executa análise de causa raiz em vulnerabilidades de segurança?

Medida 16.4 - O órgão estabelece e gerencia um inventário de componentes de software de terceiros?

Medida 16.5 - O órgão usa componentes de software de terceiros atualizados e confiáveis?

Medida 16.6 - O órgão estabelece e mantém um processo para a classificação de severidade de vulnerabilidades?

Medida 16.7 - O órgão usa modelos de configurações de segurança padrão para infraestrutura de aplicações?

Medida 16.8 - O órgão separa sistemas de produção e não produção?

Medida 16.9 - O órgão treina desenvolvedores em conceitos de segurança de aplica-

ções e codificação segura?

Medida 16.10 - O órgão aplica princípios de design seguro em arquiteturas de aplicações?

Medida 16.11 - O órgão aproveita os módulos ou serviços controlados para componentes de segurança de aplicações?

Medida 16.12 - O órgão implementa verificações de segurança em nível de código?

Medida 16.13 - O órgão realiza teste de invasão de aplicação?

Medida 16.14 - O órgão realiza a modelagem de ameaças?

Há guias de requisitos mínimos de segurança para o desenvolvimento de aplicações web, APIs e aplicações móveis disponibilizados pela SGD como material complementar [SGD 2024a]. Além disso, duas medidas são contempladas no contexto da aplicação de servidor web pelo documento *CIS NGINX Benchmark v2.1.0* [CIS 2024a]. **Das 14 medidas de segurança deste controle, 1 delas apoia uma implementação rápida pelo uso de ferramentas de software livre e será abordada na próxima seção**.

1.4. Ferramentas

Este trabalho voltará sua atenção justamente aos controles e medidas que admitem uma rápida implementação. Embora nem todas as medidas do Grupo 1 sejam abordadas aqui, as que são consideradas críticas e não envolvem adoção de políticas ou são atividades gerenciais serão trabalhadas. Ainda assim, material complementar sobre a implementação de outras medidas podem ser encontradas nos documentos dos *CIS Benchmarks* [CIS 2024a]. Das 153 medidas de segurança previstas nos *CIS Controls* e no *framework* do PPSI, entende-se que 53 são críticas e apoiam uma implementação rápida com auxílio de ferramentas de software livre. Essas 53 medidas pertencem aos controles 1–8, 10–13 e 16 e podem ser atendidas a partir da utilização das ferramentas de software livre.

1.4.1. Controle 1 - Inventário e controle de ativos corporativos

Medida 1.1. As medidas do *Framework* do PPSI relacionadas à criação de um inventário detalhado de ativos institucionais podem ser implementadas pelo **NetBox** [NetBox 2025], uma ferramenta que auxilia a gerenciar e documentar ativos, como dispositivos de rede, servidores, endereços IP, conexões de rede e outros elementos de forma eficiente e organizada. A plataforma também admite automação e integração via APIs REST (*Representational State Transfer*) e *GraphQL*, viabilizando a atualização e revisão periódica do inventário. A instalação do **NetBox** pode ser feita de forma simplificada por meio de contêineres *Docker* ou em servidores dedicados, enquanto o inventário pode ser dirigido diretamente pela interface web ou por meio de *scripts*.

Um recurso útil do **NetBox** reside em seus *webhooks*, que são acionados toda vez que um ativo é modificado. Isso viabiliza a especificação de *pipelines* que integram diferentes sistemas e ativam outros utilitários de gerenciamento de configurações, como **Ansible**, que aplicam alterações.

Medida 1.2 e 1.5. O **Kea** [ISC 2025] é uma solução moderna para o gerenciamento de endereços IP, auxiliando na atribuição dinâmica e eficiente de endereços e na coleta de

informações detalhadas sobre os dispositivos conectados à rede.

O **Kea** também oferece funcionalidades avançadas para gerenciar e registrar informações a respeito da alocação de endereços IP baseadas em *logs* DHCP, nos moldes previstos na medida 1.2 do PPSI. A ferramenta é capaz de escrever *logs* com informações sobre endereço MAC (*Media Access Control*), *hostname*, data/hora e o identificador do cliente DHCP, além de se integrar a outros serviços de gerenciamento de ativos.

Além disso, o **Kea** pode ser utilizado para implementar a medida 1.5, que exige a remoção de dispositivos não autorizados da rede, negar a conexão, e/ou colocar ativos em quarentena. Isso pode ser alcançado com as listas de controle (*allowlist/denylist*) que a aplicação utiliza para permitir ou negar concessões de endereços IP.

Medida 1.3. O **Nmap** [Lyon 2025] é uma ferramenta amplamente utilizada para a descoberta ativa e mapeamento de redes, sendo ideal para identificar dispositivos conectados a uma rede institucional. No contexto do PPSI, o **Nmap** implementa a medida 1.3, que especifica o uso de uma ferramenta de descoberta ativa configurada para executar varreduras de forma diária ou com maior frequência. Dentre as possibilidades de varredura ofercidas pelo **Nmap**, destaca-se a varredura de *ping*, que identifica *hosts* ativos na rede; a detecção de serviços, que determina quais serviços estão sendo executados e em quais portas; e a varredura com precisão, capaz de indicar sistemas operacionais e versões de software.

Medida 1.4. O **Netdiscover** [Kali 2025] é uma ferramenta simples e eficaz para a descoberta passiva de dispositivos conectados a uma rede local, podendo ser utilizado para atender às necessidades da medida 1.4, que exige a identificação de ativos na rede de forma não intrusiva. Diferentemente de ferramentas de descoberta ativa, como o **Nmap**, o **Netdiscover** opera capturando pacotes ARP (*Address Resolution Protocol*) transmitidos na rede, facilitando a determinação de dispositivos conectados sem gerar tráfego adicional significativo.

1.4.2. Controle 2 - Inventário e controle de ativos de software

Medidas 2.1 e 2.6. O **OCS Inventory** [OCS 2025] é uma solução robusta utilizada para inventário e gerenciamento de ativos de TI. Projetada para simplificar o inventário de hardware e software em redes institucionais, a ferramenta consegue automatizar a coleta de informações sobre os softwares instalados, bem como criar relatórios que categorizam e identificam os programas autorizados, não autorizados e desatualizados, seguindo as medidas 2.1 e 2.6 do PPSI. Para isso, o **OCS Inventory** conta com um agente que deve ser instalado em todo dispositivo monitorado, garantindo que as informações sejam atualizadas regularmente.

Medidas 2.3, 2.4 e 2.5. O **Security Enhanced Linux (SELinux)** [Red Hat 2025b] consiste de um módulo de segurança do *kernel* do Linux, projetado para implementar o Controle de Acesso Mandatório (MAC - *Mandatory Access Control*). Ele é responsável por restringir e regular como processos e usuários interagem com o sistema, adicionando uma camada extra de segurança contra acessos não autorizados e potenciais vulnerabilidades. No contexto do PPSI, o **SELinux** consegue definir quais programas e bibliotecas podem ser executados/carregados no sistema, atendendo às medidas 2.3 e 2.4, que exigem o con-

trole de permissões sobre softwares e bibliotecas, prevenindo execuções não autorizadas. Esse mesmo sistema também pode ser utilizado para regular o uso de *scripts*, implementando a medida 2.5.

1.4.3. Controle 3 - Proteção de Dados

Medidas 3.1, 3.2, 3.3 e 3.4. O **Apache Atlas** [Apache 2025] é uma plataforma de governança e catalogação de dados projetada para ajudar organizações a gerenciar, organizar e proteger seus dados de maneira centralizada. Ele fornece recursos avançados para rastrear metadados, gerenciar classificações de dados, criar linhagens e estabelecer políticas de governança.

Medida 3.6. O **PostgreSQL** [Citusdata 2025] é um banco de dados relacional *open-source*, conhecido por sua robustez, extensibilidade e apoio a transações *ACID* (*Atomicity, Consistency, Isolation, and Durability*). Ele admite tipos avançados (como *JSON* e *arrays*, por exemplo), índices eficientes, replicação e escalabilidade, sendo amplamente usado em aplicações críticas e modernas. Para gerenciar a retenção de dados de uma aplicação organizacional armazenados no PostgreSQL, é possível usar a extensão `pg_cron` para realizar exclusões automáticas de dados com a periodicidade desejada, de acordo com a medida 3.6 do *Framework* do PPSI.

Medida 3.7. Conhecido como o destruidor de discos, o **dd** [Sysxplore 2025] é uma ferramenta poderosa e versátil amplamente utilizada em sistemas baseados em Unix/Linux para copiar, converter e manipular dados em baixo nível. Ele opera diretamente em blocos de dados, sendo capaz de realizar operações em discos, partições, sistemas de arquivos e dispositivos de armazenamento. No contexto do PPSI, o **dd** pode desempenhar um papel importante na implementação de medidas relacionadas ao descarte seguro de dados de forma irrecuperável, garantido pela sobrescrita de dispositivos de armazenamento inteiros com dados aleatórios ou padrões específicos, em conformidade com a medida 3.7.

Medida 3.10. O **OpenSSL** [OpenSSL 2025] é uma biblioteca amplamente utilizada que fornece ferramentas para a implementação de criptografia, gerenciamento de certificados e comunicação segura em sistemas de informação. Com apoio a protocolos como TLS (*Transport Layer Security*) e SSL (*Secure Sockets Layer*), o **OpenSSL** é essencial para proteger dados em trânsito e assegurar a confidencialidade, integridade e autenticidade das comunicações. No contexto do Programa de Privacidade e Segurança da Informação, o **OpenSSL** desempenha um papel fundamental no atendimento das medidas relacionadas à proteção de dados em trânsito, principalmente na comunicação HTTPS e no gerenciamento seguro de chaves e certificados digitais.

Medidas 3.8, 3.9 e 3.11. O **LUKS** (*Linux Unified Key Setup*) [Gite 2025] é uma solução de criptografia de disco projetada para proteger dados sensíveis armazenados em dispositivos Linux. Extensivamente utilizado, o **LUKS** oferece apoio a vários algoritmos de criptografia modernos, como AES, cast5 e cast6, bem como é compatível com múltiplos sistemas de arquivos, EXT4, XFS e BTRFS. No contexto do PPSI, o **LUKS** pode ser utilizado na implementação das medidas de proteção de dados das medidas 3.8 e 3.9, dada a sua capacidade de criptografar dados em dispositivos de usuário final, como *notebooks*, *desktops* e mídias removíveis. Além disso, o **LUKS** também é uma solução eficaz para implementar a medida 3.11, que aborda a criptografia de informações críticas em

repouso, garantindo que dados armazenados em servidores e estações de trabalho estejam protegidos contra acessos não autorizados.

1.4.4. Controle 4 - Configuração segura de ativos corporativos e software

Medidas 4.4 e 4.5. O **nftables** [Red Hat 2025a] é uma ferramenta avançada de filtragem de pacotes para sistemas Linux. Ele oferece recursos avançados para a criação de tabelas, cadeias e regras personalizadas destinadas ao gerenciamento eficiente do tráfego de rede. Com essa ferramenta, é possível bloquear tráfego não autorizado enquanto somente as portas e serviços essenciais para o funcionamento normal e seguro do sistema são liberados. O **nftables** é especialmente útil na implementação das medidas 4.4 e 4.5 do *Framework* do PPSI pois auxilia na implementação e gestão de *firewalls* em servidores e dispositivos de usuários finais. Assim, com o **nftables**, por exemplo, é possível implementar uma política padrão "*deny-all*" para bloquear todo o tráfego, enquanto apenas portas específicas, como SSH (22), HTTP (80) e HTTPS (443), são liberadas.

As mesmas medidas também podem ser atentidas pelo uso da ferramenta **firewalld** [Firewalld 2025], outro recurso moderno para gerenciamento de *firewalls*. Ele oferece uma interface simplificada para configurar políticas de *firewall*, utilizando um modelo baseado em zonas para segmentar diferentes interfaces de rede e aplicar regras adaptáveis de acordo com o contexto. A ferramenta, além de admitir o uso de configurações padrão (como a política "*deny-all*"), também oferece a vantagem de liberar aplicações específicas, Essa abordagem viabiliza o controle mais granular do tráfego dentro da rede, permitindo acesso a serviços de impressão e compartilhamento de arquivos ao mesmo tempo em que mantém bloqueado todo o tráfego não autorizado.

Medida 4.7. **Ansible** [Ansible 2025] é uma ferramenta de automação de TI baseada no paradigma de Infraestrutura como Código (IaC), projetada para gerenciar configurações, implantar aplicações e orquestrar sistemas. Diferentemente de outras tecnologias, como o *SaltStack*, o **Ansible** opera sem a necessidade de agentes, utilizando conexões seguras, como SSH para sistemas baseados em Unix/Linux e WinRM para sistemas Windows. Com essa ferramenta, é possível definir uma série de *playbooks* escritos em formato *YAML*, que descrevem o estado desejado dos sistemas e automatizam tarefas repetitivas e complexas. Esses *playbooks* possibilitam que os administradores de TI implementem políticas padronizadas em toda a infraestrutura, reduzindo o risco de erros manuais e garantindo consistência operacional. Uma aplicação concreta dessa ferramenta está no gerenciamento de contas padrão, conforme definido pela medida 4.7 do PPSI. Nesse contexto, o **Ansible** facilita a automatização do controle de acesso a contas como *root*, bem como a criação, a remoção e o gerenciamento de diferentes usuários.

1.4.5. Controles 5 e 6 - Gestão de Contas e Gestão de Controle de Acesso

Medidas 5.1, 5.2, 5.4, 5.5, 5.6 e 6.2. O **FreeIPA** (*Free Identity, Policy, and Audit*) [FreeIPA 2025] é uma solução robusta para o gerenciamento de identidades e políticas de acesso que reúne diversos serviços, como *LDAP* e *Kerberos*, em uma mesma plataforma. Essa ferramenta auxilia a centralizar de forma eficiente a administração de usuários, grupos, autenticação e políticas de segurança, oferecendo uma interface simplificada para gerenciar identidades, atendendo às medidas 5.1, 5.2 e 5.5 do PPSI. O **FreeIPA** também

atende a medida 5.4 ao facilitar a criação de políticas específicas que limitam privilégios a determinados usuários ou funções, como administradores. Esse utilitário facilita a automação de processos de gestão de identidades, abrangendo a criação, modificação e desativação de contas, bem como a concessão e revogação de acessos. Além disso, viabiliza a configuração de fluxos automatizados que asseguram que novos usuários recebam os direitos apropriados, em conformidade com as medidas 5.6 e 6.2.

Uma configuração básica do **FreeIPA** parte da instalação dos pacotes necessários, seguido da execução do instalador interativo com o comando `ipa-server-install`. Durante a configuração inicial, são definidos o domínio principal, o nome do servidor e as credenciais do administrador. Após a instalação, é possível adicionar usuários e grupos, configurar políticas de acesso e definir regras como a desativação automática de contas após revogações.

Medidas 5.5, 5.6, 6.4, 6.5 e 6.6. O **Keycloak** [Keycloak 2025] é uma poderosa ferramenta de gerenciamento de identidades e acesso projetada para simplificar e aprimorar os processos de autenticação e autorização em aplicações modernas. Ele oferece uma ampla gama de recursos avançados, como autenticação centralizada e *Single Sign-On* (SSO), que possibilita aos usuários acessarem diversas aplicações com uma única autenticação. Essa ferramenta também inclui o controle de acesso baseado em funções (RBAC), que assegura uma administração granular de permissões, bem como fornece apoio à autenticação multifator (MFA). O **Keycloak** se destaca por sua capacidade de implementar autenticação centralizada (atendendo a medida 5.5), exigir autenticação multifator (atendendo as medidas 6.4, 6.5 e 6.6) e gerenciar contas e permissões de forma eficiente. Além disso, o **Keycloak** também apresenta configurações personalizadas para a desativação de contas inativas (Medida 5.6). A ferramenta é disponibilizada para distribuições Linux, conta com uma imagem oficial no *Docker Hub* e também uma implantação em *Kubernetes*.

Medidas 5.1, 5.2, 5.3, 5.6, 6.1, 6.2 e 6.3. **OpenBao** [OpenBao 2025] é uma solução avançada para o gerenciamento seguro de segredos, autenticação e políticas de controle de acesso, centralizando o armazenamento de credenciais, como senhas, tokens, certificados e chaves de API, em um ambiente seguro, garantindo que segredos sejam acessados e gerenciados de forma controlada e auditável. Ele também oferece apoio à geração dinâmica de senhas únicas e *tokens*, garantindo que credenciais sejam sempre exclusivas, com uso de autenticação multifator (MFA) e controle de acesso baseado em politicas (RBAC). Além disso, o **OpenBao** facilita a revogação de acessos por meio da desativação automática de segredos expirados ou desnecessários, de acordo com as políticas configuradas.

A ferramenta é compatível com as principais distribuições Linux e pode ser facilmente implantado em ambientes baseados em contêineres, utilizando o *Docker* para simplificar a configuração e a escalabilidade.

1.4.6. Controle 7 - Gestão Contínua de Vulnerabilidades

Medidas 7.1 e 7.2. As medidas 7.1 e 7.2 do *Framework* do PPSI tratam sobre a varredura automatizada dos ativos institucionais para descoberta de vulnerabilidades. Essa atividade pode ser apoiada pelo uso do **OpenVAS** (*Open Vulnerability Assessment Scanner*), um mecanismo de varredura que executa Testes de Vulnerabilidade (VTs) nos sistemas-alvo utilizando informações adquiridas a partir de um *feed* atualizado diariamente. O

OpenVAS suporta testes de vulnerabilidade autenticados e não autenticados, testes em protocolos de rede de alto e baixo nível e testes customizados [Greenbone 2025b].

A instalação da ferramenta pode ser simplificada pelo uso de um contêiner *Docker* disponibilizado na página de documentação da ferramenta [Greenbone 2025a] e possui interface gráfica, possibilitando o uso facilitado de suas funcionalidades. A varredura parte da seleção da faixa de rede a ser escaneada, o horário de início e inserção opcional de credenciais, seguindo para a verificação de vulnerabilidades nos *hosts* encontrados. A primeira execução da ferramenta demanda uma sincronização inicial do *feed* de testes, o que pode levar de 15 a 45 minutos e precisa ser feita antes da primeira varredura. Os resultados obtidos pela varredura são exibidos em um relatório que indica as vulnerabilidades encontradas, o grau de severidade delas e formas de correção. A ferramenta também suporta o agendamento de varreduras, cumprindo o que estabelece as medidas de segurança 7.1 e 7.2.

1.4.7. Controle 8 - Gestão de registros de auditoria

Medida 8.3. O **Chrony** [Chrony 2024] é um serviço de sincronização de tempo para sistemas operacionais baseados em Linux, projetado para substituir o tradicional NTP (*Network Time Protocol*). Ele é ideal para ambientes modernos, oferecendo uma solução eficiente, rápida e precisa para manter os relógios dos sistemas sincronizados e de acordo com a medida 8.3 do *Framework* do PPSI.

Medidas 8.5, 8.6 e 8.9. O **auditd** [Grubb 2024] é uma ferramenta de auditoria no Linux que registra eventos de segurança, como execução de comandos e alterações no sistema. Ele viabiliza monitorar atividades de usuários e processos, ajudando a detectar comportamentos maliciosos e a garantir conformidade com políticas de segurança. As principais ferramentas são `auditctl` (para gerenciar regras), `ausearch` (para buscar `logs`) e `aureport` (para gerar relatórios).

1.4.8. Controle 10 - Defesas contra Malware

Medidas 10.1 e 10.2. O **ClamAV** [ClamAV 2025] é um antivírus de código aberto, projetado para detectar *malwares* como vírus, *trojans* e *worms*. Ele suporta múltiplos formatos de arquivos, incluindo compactados, e realiza varreduras em tempo real ou sob demanda. É amplamente utilizado em servidores de e-mail e arquivos e é compatível com Linux, macOS e Windows. Seus principais componentes são: (a) `clamscan` para varreduras manuais de arquivos; (b) `freshclam` para atualização automática de assinaturas; e (c) `clamd`, que oferece varredura contínua de arquivos.

É possível usar o `clamscan` para fazer a varredura do todos os arquivos do sistema, o *daemon* `clamd` para varreduras em segundo plano e o `freshclam` para atualizar o banco de assinaturas automaticamente. Para realizar varreduras em e-mails, é possível usar o `amavis` junto com o **ClamAV**. O `amavis` é um filtro de conteúdo de e-mail, utilizado para integrar verificações de vírus e outros tipos de escaneamento (como antivírus, spam, etc.) em servidores de e-mail. Ele funciona como um intermediário entre um servidor de e-mail e programas de verificação de conteúdo, como o **ClamAV**. Para fazer essa ligação, o `amavisd` deve se conectar com o socket do `clamd`.

1.4.9. Controle 11 - Recuperação de dados

Medidas 11.1, 11.3, 11.4 e 11.5. O **Bacula** [Bacula 2025] é uma solução robusta e modular para o gerenciamento de *backups*, recuperação e verificação de dados. Projetado para suportar múltiplos sistemas operacionais, como Linux, Windows e MacOS, o **Bacula** oferece compatibilidade com diversos tipos de armazenamento, incluindo discos locais, fitas magnéticas e serviços de armazenamento na nuvem.

No contexto do PPSI, o **Bacula** pode desempenhar um papel central no atendimento às medidas do Controle 11, relacionadas à recuperação e backup de dados. A ferramenta, por exemplo, facilita a execução de *backups* automatizados (medida 11.3), garantindo que os dados críticos da organização sejam salvos regularmente. Além disso, o **Bacula** propicia a criação de instâncias isoladas para armazenamento de dados de recuperação (medida 11.4), como *backups* em dispositivos off-line, locais remotos ou na nuvem. Adicionalmente, o **Bacula** oferece suporte à criptografia de dados em trânsito e em repouso, atendendo à medida 11.1, que exige a proteção adequada dos dados de recuperação. Por fim, essa ferramenta é capaz de realizar testes regulares de integridade e recuperação (medida 11.5), sendo possível verificar a usabilidade dos *backups* e garantindo que os dados possam ser restaurados corretamente em caso de necessidade.

1.4.10. Controle 12 - Gestão da infraestrutura de rede

Medida 12.1. O **PlantUML** [PlantUML 2025] é uma ferramenta avançada para a criação de diagramas a partir de texto, amplamente acessível em diversas plataformas e ferramentas modernas, como IDEs (*Integrated Development Environment*), sistemas de controle de versão e editores de texto. Ele oferece recursos poderosos para a geração de diagramas de sequência, classes, casos de uso e muitos outros, de forma eficiente e personalizável. Com essa ferramenta, é possível documentar sistemas complexos de maneira clara e estruturada, garantindo que equipes de desenvolvimento e *stakeholders* compreendam e mantenham a arquitetura e os fluxos de trabalho com facilidade. Portanto, o **PlantUML** é uma ferramenta especialmente útil para atender à medida 12.1 do PPSI, que recomenda elaborar e manter diagramas da arquitetura de rede.

1.4.11. Controle 13 - Monitoramento e defesa da Rede

Medida 13.6. Para tratar da filtragem na camada de aplicação prevista na medida 13.6, pode-se utilizar ferramentas do tipo WAF (*Web Application Firewall*), como o **open-appsec**, para realizar a filtragem de requisições que um servidor web NGINX recebe. O **open-appsec** é um software livre e possui planos gratuitos básicos, mas capazes de detectar e prevenir ataques Web baseado em técnicas de *machine-learning* e ataques contra APIs. Por utilizar fundamentos de *machine-learning*, este software é capaz de detectar os principais ataques da OWASP Top 10 (*Open Worldwide Application Security Project*) e também ataques *0-day*.Documentos sobre a instalação, uso e visualização de alertas da ferramenta podem ser verificados na sua página na internet [CheckPoint 2025]. Outra opção de WAF é **Modsecurity**, uma extensão para o serviço NGINX capaz de filtrar requisições HTTP [Zimmerle and Belov 2024].

Medida 13.8. O **AIDE** (*Advanced Intrusion Detection Environment*) é uma ferramenta de software livre capaz de checar e monitorar a integridade de arquivos e diretórios dentro de

sistemas Linux, oferecendo recursos como verificação de atributos de arquivos, checagem de múltiplos *checksums*, arquivos de configuração e banco de dados em texto simples, além de admitir o uso de expressões regulares para personalizar o que será monitorado.O **AIDE** é software livre, disponível no *github* [AIDE 2025]. A ferramenta está incluída em várias distribuições Linux, como Debian, Ubuntu, FreeBSD, Gentoo e outros, podendo ser instalado a partir da linha de comando. As configurações da ferramenta se encontram no arquivo `aide.conf` localizado em `/etc/aide` e é neste documento que se indica os arquivos e diretórios monitorados [Kastning 2024]. O uso da ferramenta ocorre por meio da linha de comando do sistema operacional e sua automatização pode ser feita por meio do utilitário `cron` do Linux. As checagens podem ser feitas diariamente, enquanto novos bancos de dados podem ser criados semanalmente. A capacidade de verificar a alteração não autorizada em arquivos e diretórios do sistema se adequa à medida de segurança 13.3 do *framework* do PPSI, detectando ataques ao *host*.

Medida 13.9. O **Suricata** [Suricata 2025] é uma conhecida ferramenta desenvolvida para ser um mecanismo de detecção de intrusão moderno, aproveitando de arquiteturas *multi-thread* nativamente. O funcionamento do Suricata é baseado na criação de regras compostas por ações, cabeçalho dos protocolos de rede e opções extras. As ações podem ser dos tipos `alert` (que gera um alerta), `pass` (que interrompe a inspeção adicional do pacote), `drop` (que descarta o pacote e gera um alerta) e `reject` (que responde um pacote com *flag* RST). O Suricata também suporta os protocolos de rede e de aplicação, como TCP, UDP, ICMP, HTTP, SSH e FTP, dentre outros [Bueno 2024]. A ferramenta pode ser instalada a partir da linha de comando na maioria das distribuições Linux, e suas configurações podem incluir indicações das interfaces de rede que capturarão pacotes, regras a serem importadas, formatos dos *logs*, etc. As funções da ferramenta Suricata são capazes de implementar a medida 13.4 do *framework* do PPSI, fornecendo uma possibilidade de implementação de sistema de detecção de intrusão de rede.

1.4.12. Controle 16 - Segurança de aplicações

Medida 16.4. A atividade de estabelecer e gerenciar um inventário de componentes de software de terceiros é facilitada pela extração de um **SBOM** (*software bill of materials*). A plataforma de versionamento de código **Github** disponibiliza um utilitário para todos os seus usuários que possibilita a extração de um relatório de componentes a partir de um repositório [Github 2025].

Medida 16.8. O **OpenTofu** [OpenTofu 2025] é uma ferramenta de Infraestrutura como Código (IaC) de código aberto que possibilita criar, gerenciar e versionar infraestrutura de maneira declarativa. Ele oferece uma alternativa totalmente aberta, com foco na comunidade, para gerenciar infraestrutura em nuvem e ambientes *on-premises*. Semelhante ao *Terraform*, o *OpenTofu* utiliza uma abordagem declarativa e configurações em HCL *(HashiCorp Configuration Language)* para descrever a infraestrutura.

A medida 16.8 do PPSI enfatiza a separação entre sistemas de produção e não produção, promovendo estabilidade e segurança. O uso conjunto do **OpenTofu** e **Ansible** auxilia no cumprimento dessa exigência ao tornar a infraestrutura reproduzível e consistente. O **OpenTofu** contribui automatizando a criação e a destruição de ambientes, enquanto o **Ansible** contribui automatizando configurações específicas de um serviço

dentro de cada ambiente criado. Ao combinar o uso das ferramentas **OpenTofu** e **Ansible**, a separação entre ambientes é garantida.

1.5. Conclusão

Implementar controles e medidas de segurança previstas em *frameworks* pode ser uma tarefa complexa, principalmente para entidades que não possuem políticas e procedimentos de segurança bem definidos. A fim de evitar medidas de cunho gerencial e focando em atividades práticas de rápida implementação, este trabalho buscou fornecer uma base sólida para que as organizações possam dar seus primeiros passos em direção à conformidade com o uso de software livre. Entende-se que a implementação das medidas aqui abordadas possibilita alcançar um patamar satisfatório de cibersegurança no contexto dessas organizações.

Referências

[AIDE 2025] AIDE (2025). Aide. https://github.com/aide/aide.

[Ansible 2025] Ansible (2025). Ansible documentation. https://docs.ansible.com/.

[Apache 2025] Apache (2025). Apache atlas quick start. https://atlas.apache.org/#/QuickStart.

[Bacula 2025] Bacula (2025). Bacula systems backup software main manual 15.0.x. https://www.bacula.org/15.0.x-manuals/en/main/index.html.

[Bueno 2024] Bueno, C. I. (2024). Um estudo de caso sobre a implantação de um sistema de detecção de intrusões aplicado a um projeto em parceria com o sus. Trabalho de Conclusão de Curso.

[CheckPoint 2025] CheckPoint (2025). Getting started. https://docs.openappsec.io/getting-started/getting-started.

[Chrony 2024] Chrony (2024). Chrony homepage. https://chrony-project.org/.

[CIS 2024a] CIS (2024a). Cis benchmarks. https://learn.cisecurity.org/benchmarks.

[CIS 2024b] CIS (2024b). Cis benchmarks overview. https://www.cisecurity.org/cis-benchmarks-overview.

[CIS 2024c] CIS (2024c). Cis critical security controls implementation. https://www.cisecurity.org/controls/implementation-groups/.

[CIS 2024d] CIS (2024d). Cis critical security controls implementation group 2. https://www.cisecurity.org/controls/implementation-groups/ig3.

[CIS 2024e] CIS (2024e). Cis critical security controls navigator. https://www.cisecurity.org/controls/cis-controls-navigator.

[CIS 2024f] CIS (2024f). Cis critical security controls version 8.1.

[CIS 2024g] CIS (2024g). Mapping and compliance. https://www.cisecurity.org/cybersecurity-tools/mapping-compliance.

[Citusdata 2025] Citusdata (2025). pg_cron github. https://github.com/citusdata/pg_cron.

[ClamAV 2025] ClamAV (2025). Clamav. https://www.clamav.net/.

[Firewalld 2025] Firewalld (2025). Firewalld documentation. https://firewalld.org/documentation/.

[FreeIPA 2025] FreeIPA (2025). Freeipa quick start guide. https://www.freeipa.org/page/Quick_Start_Guide.

[Gite 2025] Gite, V. (2025). How to: Linux hard disk encryption with luks cryptsetup command. https://www.cyberciti.biz/security/howto-linux-hard-disk-encryption-with-luks-cryptsetup-command/.

[Github 2025] Github (2025). Como exportar uma lista de materiais de software para seu repositório. https://docs.github.com/pt/code-security/supply-chain-security/understanding-your-software-supply-chain/exporting-a-software-bill-of-materials-for-your-repository.

[Greenbone 2025a] Greenbone (2025a). Greenbone community containers. https://greenbone.github.io/docs/latest/22.4/container/.

[Greenbone 2025b] Greenbone (2025b). Greenbone openvas. https://www.openvas.org/.

[Grubb 2024] Grubb, S. (2024). auditd(8) - linux man page. https://linux.die.net/man/8/auditd/.

[IBM 2024] IBM (2024). What is shadow it? https://www.ibm.com/topics/shadow-it.

[ISC 2025] ISC, I. S. C. (2025). Kea dhcp documentation - version 2.6.1. https://kea.readthedocs.io/en/kea-2.6.1/.

[Kali 2025] Kali (2025). Netdiscover - kali linux tools. https://www.kali.org/tools/netdiscover/.

[Kastning 2024] Kastning, J. (2024). Introduction to the advanced intrusion detection environment (aide). https://www.opensourcerers.org/2024/04/15/introduction-to-the-advanced-intrusion-detection-environment-aide/.

[Keycloak 2025] Keycloak (2025). Keycloak server administration guide (latest version). https://www.keycloak.org/docs/latest/server_admin/index.html.

[Lyon 2025] Lyon, G. (2025). Nmap homepage. https://nmap.org/.

[NetBox 2025] NetBox (2025). Netbox documentation (stable version). https://netboxlabs.com/docs/netbox/en/stable/.

[NIST 2024a] NIST (2024a). About us. https://www.nist.gov/about-nist.

[NIST 2024b] NIST (2024b). Cybersecurity. https://www.nist.gov/cybersecurity.

[NIST 2024c] NIST (2024c). Nist csf 2.0 implementation examples. https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf.

[NIST 2024d] NIST (2024d). Nist cybersecurity framework 2.0: Small business quick-start guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf.

[NIST 2024e] NIST (2024e). The nist cybersecurity framework (csf) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[NIST 2024f] NIST (2024f). Node-link diagram of the cybersecurity framework v2.0 mapped to controls. https://csf.tools/visualizations/node-link-diagram-of-the-cybersecurity-framework-v2-0-mapped-to-controls/.

[NIST 2024g] NIST (2024g). Topics. https://www.nist.gov/topics.

[OCS 2025] OCS (2025). Ocs inventory ng wiki. https://wiki.ocsinventory-ng.org/.

[OpenBao 2025] OpenBao (2025). Openbao documentation. https://openbao.org/docs/.

[OpenSSL 2025] OpenSSL (2025). Openssl library. https://linux.die.net/man/1/openssl.

[OpenTofu 2025] OpenTofu (2025). Opentofu. https://opentofu.org/.

[PlantUML 2025] PlantUML (2025). Plantuml nwdiag. https://plantuml.com/nwdiag.

[Red Hat 2025a] Red Hat, I. (2025a). Getting started with nftables - configuring and managing networking - red hat enterprise linux 8. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/getting-started-with-nftables_configuring-and-managing-networking#getting-started-with-nftables_configuring-and-managing-networking.

[Red Hat 2025b] Red Hat, I. (2025b). Selinux users and administrators guide - red hat enterprise linux 7. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index#idm140415566801680.

[SGD 2023a] SGD (2023a). Cartilha do programa de privacidade e segurança da informação (ppsi). https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908.

[SGD 2023b] SGD (2023b). Portaria sgd/mgi nº 852, de 28 de marÇo de 2023. https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908.

[SGD 2024a] SGD (2024a). Framework, guias e modelos. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos.

[SGD 2024b] SGD (2024b). Guia do framework de privacidade e segurança da informação. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf.

[Suricata 2025] Suricata (2025). Suricata homepage. https://suricata.io/.

[Sysxplore 2025] Sysxplore (2025). The complete guide to the dd command in linux. https://blog.kubesimplify.com/the-complete-guide-to-the-dd-command-in-linux.

[Zimmerle and Belov 2024] Zimmerle, F. and Belov, A. (2024). Modsecurity-nginx. https://github.com/owasp-modsecurity/ModSecurity-nginx.