UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E BIOLÓGICAS
DEPARTAMENTO DE COMPUTAÇÃO

GUILHERME FERREIRA ROCHA
Orientador: Prof. Dr. Carlos Frederico Marcelo da Cunha Cavalcanti

LIMITANDO VULNERABILIDADES DE SISTEMAS OPERACIONAIS COM ANSIBLE E CIS CONTROLS

Ouro Preto, MG
2024

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E BIOLÓGICAS
DEPARTAMENTO DE COMPUTAÇÃO

GUILHERME FERREIRA ROCHA

LIMITANDO VULNERABILIDADES DE SISTEMAS OPERACIONAIS COM ANSIBLE E CIS CONTROLS

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal de Ouro Preto como parte dos requisitos necessários para a obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Carlos Frederico Marcelo da Cunha Cavalcanti

Ouro Preto, MG
2024

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
DEPARTAMENTO DE COMPUTACAO

FOLHA DE APROVAÇÃO

Guilherme Ferreira Rocha

LIMITANDO VULNERABILIDADES DE SISTEMAS OPERACIONAIS COM ANSIBLE E CIS CONTROLS

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Ciência da Computação

Aprovada em 21 de Outubro de 2024.

Membros da banca

Carlos Frederico M. da Cunha Cavalcanti (Orientador) - Doutor - Universidade Federal de Ouro Preto
Fernando Cortez Sica (Examinador) - Doutor - Universidade Federal de Ouro Preto
Ricardo Augusto Rabelo Oliveira (Examinador) - Doutor - Universidade Federal de Ouro Preto

Carlos Frederico M. da Cunha Cavalcanti, Orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 12/11/2024.

Documento assinado eletronicamente por **Carlos Frederico Marcelo da Cunha Cavalcanti**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 13/11/2024, às 11:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0795430** e o código CRC **B5FEC68D**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: 3135591692 - www.ufop.br

Resumo

O trabalho consiste em uma pesquisa experimental, que tem como objetivo a implementação de uma abordagem automatizada para mitigar vulnerabilidades em sistemas operacionais, utilizando a ferramenta *Ansible* e o *framework CIS Benchmark* como base. A preciosidade dos dados nos dias atuais é justificativa para a implementação de medidas de segurança nas empresas. Os objetivos específicos incluíram o estudo de padrões/ *frameworks* de segurança, a implementação de uma prova de conceito para as configurações automatizadas, e a mensuração da evolução do sistema após a implementação. A metodologia adotada envolveu a execução da ferramenta *CIS-CAT Lite* para avaliar a conformidade dos controles recomendados pelo *Benchmark*, resultando em uma pontuação que evoluiu de 22% para 24%. Os resultados parciais demonstraram a viabilidade da abordagem automatizada, com 11 dos 381 controles sendo configurados por automação. Além disso, foram desenvolvidos fluxos de trabalho no n8n para exemplificar a aplicação prática das automações em cenários empresariais, integrando o Ansible e o CIS-CAT a diversas plataformas de comunicação, bancos de dados e sistemas de gerenciamento de serviços de TI (*ITSM*). Esses fluxos demonstraram como a automação pode ser adaptada às necessidades específicas de cada organização, otimizando a execução de configurações de segurança e melhorando a eficiência operacional. Foram apontados trabalhos futuros e possíveis melhorias, como a implementação dos 79 controles que representam a higiene básica de segurança e a adição de outros tipos de testes de vulnerabilidade. Concluiu-se que a automação de configurações de segurança é valiosa para reduzir o tempo operacional na implementação de controles, e que a abordagem automatizada, combinada com fluxos de trabalho dinâmicos como os do n8n, é crucial para fortalecer a segurança dos sistemas e promover eficiência e confiabilidade nas operações empresariais, reforçando a importância contínua da pesquisa nesse contexto acadêmico.

Palavras-chave: Vulnerabilidades. Sistema Operacional. Automação. *Ansible. CIS Controls.* Padrões de segurança. Fluxos de trabalho. N8N.

Abstract

This work consists of an experimental study aimed at implementing an automated approach to mitigate vulnerabilities in operating systems, using the *Ansible* tool and the *CIS Benchmark* framework as the foundation. The critical importance of data in today's world justifies the implementation of security measures within companies. The specific objectives included studying security standards/*frameworks*, implementing a proof of concept for automated configurations, and measuring the evolution of the system after implementation. The adopted methodology involved executing the *CIS-CAT Lite* tool to assess compliance with the controls recommended by the *Benchmark*, resulting in a score that improved from 22% to 24%. Partial results demonstrated the feasibility of the automated approach, with 11 out of 381 controls being configured through automation. Additionally, n8n workflows were developed to illustrate the practical application of automations in business scenarios, integrating Ansible and CIS-CAT with various communication platforms, databases, and IT service management (*ITSM*) systems. These workflows demonstrated how automation can be tailored to the specific needs of each organization, optimizing the execution of security configurations and enhancing operational efficiency. Future work and potential improvements were identified, such as the implementation of the 79 controls that represent basic security hygiene and the addition of other types of vulnerability testing. The study concluded that automating security configurations is valuable for reducing operational time in implementing controls, and that the automated approach, combined with dynamic workflows like those in n8n, is crucial for strengthening system security and promoting efficiency and reliability in business operations, reinforcing the ongoing importance of research in this academic context.

Keywords: Vulnerabilities. Operational system. Automation. Ansible. CIS Controls. Security standards. Workflows. N8N.

Lista de Abreviaturas e Siglas

ABNT	Associação Brasileira de Normas Técnicas
DECOM	Departamento de Computação
UFOP	Universidade Federal de Ouro Preto
SO	Sistema Operacional
TI	Tecnologia da Informação
CIS	Center for Internet Security
IG	Grupos de implementação, do inglês Implementation Groups
IoT	Internet das Coisas, do inglês Internet of Things
ITSM	Sistemas de gerenciamento de TI, do inglês IT Service Management

Sumário

1 Introdução

1.1 Justificativa

Atualmente, é discutível que os dados são os bens mais preciosos para os negócios mundiais. A informação é o impulso para a competitividade e diferencial de mercado, servindo como base para decisões precisas e assertivas. Com isso, a segurança da informação ganha força conforme a modernização e evolução dos processos empresariais pois seu objetivo é definido em 3 pilares, sendo eles a preservação da Confidencialidade, Integridade e Disponibilidade das informações.

Para proteger informações críticas, é essencial implantar medidas de segurança nos sistemas que as armazenam. Essas medidas ajudam a reduzir as vulnerabilidades que poderiam ser exploradas em casos de roubo de dados. Essa abordagem não apenas impede acessos não autorizados, mas também responde de maneira proativa a possíveis ameaças, tornando os sistemas mais resistentes perante a segurança cibernética. Esse foco estratégico na prevenção e resposta a incidentes é fundamental para apoiar os 3 pilares, fortalecendo a postura geral de segurança da organização.

O êxito na implementação de medidas de proteção contra vulnerabilidades está diretamente ligado à escolha criteriosa de um guia de configurações e ações adequado. Dada a complexidade e a diversidade de tecnologias, protocolos, aplicações e vulnerabilidades presentes nos sistemas, a seleção de um guia abrangente e adaptável é fundamental para enfrentar as ameaças em constante evolução da segurança cibernética. Além disso, a eficácia dessas medidas é potencializada pela implementação de uma automação replicável e escalável. Esse aspecto é crucial para alinhar as práticas de segurança aos processos específicos das empresas, personalizando-as conforme suas necessidades e escalas. Ao mitigar falhas humanas e garantir consistência operacional, essa abordagem não apenas fortalece a segurança dos sistemas, mas também promove a eficiência e a confiabilidade nas operações empresariais.

1.2 Objetivos

O objetivo geral deste trabalho é a implementação de uma abordagem automatizada destinada a mitigar vulnerabilidades conhecidas em sistemas operacionais e reduzir riscos de acessos não autorizados por meio do *Hardening* de máquinas. Essa iniciativa se fundamenta na adoção de um *framework* ou guia amplamente reconhecido no cenário de segurança cibernética, que sejam práticos e aplicáveis em ciclos de desenvolvimento da empresa. Este objetivo reflete o compromisso em contribuir para a eficácia das estratégias de segurança, proporcionando uma

abordagem automatizada, sistemática e robusta para a limitação de vulnerabilidades em ambientes operacionais.

Os objetivos específicos são:

- Estudar sobre padrões/ *frameworks* de segurança e *Hardening*;
- Definir o padrão/ *framework* de mercado a ser adotado;
- Definir a tecnologia de automação capaz de realizar as configurações necessárias no sistema operacional;
- Propor uma prova de conceito para realizar as configurações automatizadas de *Hardening* do sistema;
- Implementar uma estrutura replicável e organizada de código das configurações, facilitando a implantação, manutenção e registros de auditoria;
- Mensurar a evolução do sistema, levando em conta o ponto de início e o ponto após as configurações serem realizadas de forma automatizada;

1.3 Organização do Trabalho

A estrutura deste trabalho segue a seguinte organização. Na seção 2, são descritos os principais conceitos e princípios vinculados à Segurança da Informação, vulnerabilidades e automação, incluindo uma revisão de trabalhos correlatos que enriquecem a compreensão da proposta de pesquisa. A metodologia adotada para este estudo é detalhada na seção 3. A seção 4 destaca os resultados parciais obtidos durante a condução desta pesquisa. Por fim, na seção 5, são apresentadas as considerações finais, além de indicar possíveis direções para o prosseguimento deste trabalho.

2 Revisão Bibliográfica

2.1 Fundamentação Teórica

A Segurança da Informação é um campo estratégico dedicado à proteção, preservação e gerenciamento adequado dos dados de uma organização. Este domínio abrange a implementação de medidas e políticas destinadas a assegurar a Confidencialidade, Integridade e Disponibilidade das informações. A Confidencialidade refere-se à garantia de que apenas indivíduos autorizados têm acesso a informações sensíveis, evitando divulgação não autorizada. A Integridade visa preservar a precisão e a completude dos dados, prevenindo alterações não autorizadas ou corrupção. Por fim, a Disponibilidade assegura que as informações estejam acessíveis quando necessário, evitando interrupções indesejadas. Esses princípios fundamentais são a base essencial da Segurança da Informação, proporcionando uma estrutura sólida para garantir a proteção dos dados e a continuidade operacional das organizações (Solms; Solms, 2018).

2.1.1 Sistemas Operacionais e Vulnerabilidades

Sistemas operacionais(SO) são programas(*Softwares*) fundamentais que atuam como uma interface entre o *hardware* de um dispositivo de computação e o usuário. Esses *softwares* gerenciam recursos do sistema, são responsáveis pelo controle e coordenação de tarefas, manipulação de entrada e saída, facilitam a execução de outros programas e atuam como um mediador visual, humanizado e eficiente para o usuário final, além de garantir a segurança e estabilidade do ambiente computacional (Oliveira; Carissimi; Toscani, 2001).

Os sistemas operacionais desempenham um papel crítico nas empresas de tecnologia da informação, abrangendo desde os dispositivos utilizados por colaboradores até os servidores nos quais suas aplicações são executadas. A escolha dos sistemas operacionais adotados pela empresa é influenciada por fatores como a produtividade dos colaboradores, parcerias comerciais e a finalidade do produto. No entanto, é crucial considerar as potenciais vulnerabilidades em cada sistema, bem como a abordagem para mitigar esses riscos. A implementação de políticas específicas em torno dessas questões de segurança torna-se essencial para prevenir e reduzir a ocorrência de incidentes de segurança, garantindo a robustez e integridade dos ambientes tecnológicos empresariais.

Entre as vulnerabilidades mais comuns encontradas em sistemas operacionais, destacam-se falhas de segurança no *kernel*, que servem como o núcleo central do sistema, e vulnerabilidades em serviços e processos em execução. Os ofensores podem se aproveitar da deficiência em configurações do sistema, falta de atualizações de segurança, e também da falta de conhecimento do próprio usuário, que pode ser induzido a instalar *softwares* maliciosos que exploram as

fraquezas citadas para comprometer a integridade dos dados e a operação do sistema (Sharma; Kumar; Sharma, 2011).

2.1.2 Automação de Provisionamento de Ativos

Os ativos empresariais englobam elementos essenciais, tanto materiais quanto abstratos, que desempenham um papel fundamental no pleno funcionamento de uma organização. No contexto tecnológico empresarial, esses ativos abrangem uma ampla gama de elementos, como infraestrutura de TI, máquinas virtuais que hospedam aplicações, computadores e dispositivos móveis dos funcionários, *softwares* de outras empresas para utilização, produtividade, registro de informações pelos funcionários, entre outros aspectos essenciais para a eficiência operacional. Esses ativos empresariais não apenas facilitam as operações diárias, mas também representam investimentos estratégicos que contribuem para a produtividade, a inovação e o sucesso global da organização. A gestão eficaz desses ativos, considerando sua segurança, atualização e otimização contínua, é crucial para garantir o desempenho consistente, a resiliência das operações e a constante evolução do negócio (Vion, 2018).

Ao automatizar o processo de provisionamento de ativos, a organização estabelece uma base sólida de consistência, padrões, redução da probabilidade de erros humanos, facilidade de manutenção e auditoria dos sistemas, provendo assim um ambiente tecnológico mais estável, eficiente e seguro. No âmbito da nuvem e infraestrutura, o provisionamento automatizado de pacotes e configurações é essencial para garantir a eficácia, escalabilidade e consistência das operações. Por exemplo, no contexto de aplicações *web*, a automação configura parâmetros críticos, tais como pacotes necessários para execução, rede e segurança do sistema, capacidade e componentes de *hardware*, distribuição e balanceamento de carga, entre outras configurações, permitindo que estas operem de maneira otimizada e segura (McAllister, 2017). Em relação aos computadores dos funcionários, a automação assume a forma de configurações padronizadas de segurança, instalação automatizada de aplicativos essenciais para o dia a dia de trabalho, atribuição de licenças, configurações de atalhos e ajustes de rede. Esses processos automáticos não apenas aceleram a integração de novos dispositivos, mas também garantem que cada computador de funcionário seja configurado de maneira consistente, promovendo eficiência operacional e conformidade com políticas de segurança estabelecidas pela organização.

2.1.3 Limitação de Vulnerabilidades e Padrões de segurança

Embora seja uma realidade incontestável que não é possível conhecer e mitigar todas as potenciais vulnerabilidades de um sistema, restringir proativamente e limitar aquelas já conhecidas é de extrema importância. A fortificação de um sistema é chamada de *Hardening*, que refere-se à prática de aprimorar a segurança de um sistema operacional por meio da configuração cuidadosa de parâmetros e políticas. Isso inclui a desativação de serviços não essenciais, a aplicação rigorosa de políticas de controle de acesso e a implementação de configurações de segurança

robustas. Estratégias eficazes para limitar vulnerabilidades envolvem a análise regular e proativa de possíveis pontos de falha, a aplicação consistente de atualizações (*patches*) de segurança e a configuração de políticas que restringem acessos não autorizados. O controle de acesso e políticas de segurança são peças-chave nesse processo, determinando quem tem permissão para acessar quais recursos e definindo regras claras para o uso seguro do sistema (Ferreira, 2021).

Em meio ao cenário complexo e dinâmico da segurança cibernética, a adoção de normas e padrões reconhecidos internacionalmente torna-se fundamental para garantir a proteção efetiva dos computadores corporativos e mostrar maturidade para seus clientes. Diversos padrões, como ISO/IEC 27001, *NIST Cybersecurity Framework* e *CIS Controls*, estabelecem diretrizes abrangentes para a implementação de práticas de segurança robustas. Cada um destes padrões apresenta abordagens distintas, refletindo diferentes perspectivas e requisitos, desde a conformidade regulatória até a resiliência contra ameaças específicas (Bashofi; Salman, 2022).

2.1.4 CIS Controls e CIS Benchmark

O *Center for Internet Security* (CIS) é uma organização sem fins lucrativos que utiliza o poder de uma comunidade global de tecnologia da informação para proteger organizações públicas e privadas contra ameaças cibernéticas (CIS…, b). Para isso a organização desenvolve e propõe melhores práticas, padrões e diretrizes que fortaleçam a cultura de segurança de empresas em todo o mundo. Os recursos oferecidos pelo CIS possuem uma abordagem orientada a ação, que é de grande valia para o negócio, proporcionado uma postura mais resiliente e reativa em relação às ameaças cibernéticas, protegendo não apenas os ativos da empresa, mas também sua reputação e confiança perante os clientes.

Um dos produtos do CIS é justamente o *CIS Controls*, que documenta um conjunto prescrito, priorizado e simplificado de práticas que podem guiar uma empresa a fortalecer suas estruturas de cibersegurança. Os controles contidos no documento são projetados para serem práticos, acionáveis e fáceis de implementar, mesmo para organizações com recursos limitados. Eles são baseados nas ameaças mais comuns presentes no mundo da tecnologia da informação, indicando práticas mais eficazes para mitigar essas ameaças (CIS…, d).

No momento que este trabalho foi escrito, a versão mais recente é a oitava (CIS Controls v8) publicada em Maio de 2021. Esse documento possui 18 controles (Fig. 2.1) que internamente são divididos em medidas de segurança, ou também chamados de sub-controles. No total, possuindo 153 medidas de segurança dentre os 18 controles. Os controles são divididos em 3 Grupos de Implementação (IG - do inglês *Implementation Groups*), sendo eles, o IG1, IG2 e IG3, considerando o primeiro o mais básico e terceiro o mais avançado, onde os mais avançados incluem a implementação dos mais básicos (Fig. 2.2). Essa divisão foi feita a partir da versão 7.1, devido a grande quantidade de sub-controles, para que, dessa forma, organizações menores podem começar implementando o primeiro grupo de medidas e ir avançando conforme necessidade, maturidade e crescimento da empresa (CIS…, c).

Figura 2.1 – Lista de controles da versão 8 do CIS Controls.

Figura 2.2 – Grupos de implementação do CIS Controls.

A organização CIS publicou também diversos guias de aplicações práticas do *CIS Controls* em ambientes específicos, chamados de *CIS Benchmarks*. Eles concentram-se em configurações técnicas dentro da tecnologia abordada, onde cada recomendação de configuração do *CIS Benchmark* tem sua respectiva medida de segurança do *CIS Controls* associada a ela, assim como o seu grupo de implementação. Os variados *Benchmarks* já publicados abordam tecnologias como sistemas operacionais, navegadores de internet, ambientes de nuvem, dispositivos móveis, entre outros (CIS..., a).

2.1.5 Ansible na Segurança de Sistemas Operacionais

As ferramentas de automação e orquestração desempenham um papel fundamental na evolução e eficiência dos ambientes tecnológicos das organizações. No cenário da tecnologia da informação, a automação se refere à capacidade de realizar tarefas rotineiras de maneira programada, reduzindo a intervenção manual humana e aumentando a consistência operacional.

O *Ansible* emprega uma abordagem declarativa para o gerenciamento de configuração, permitindo que os usuários definam o estado desejado de seus sistemas, em vez de detalhar os passos para alcançar esse estado. Isso é realizado por meio do uso de *playbooks*, que são arquivos *YAML* que descrevem as tarefas a serem executadas em máquinas-alvo. O *Ansible* opera de maneira sem agente, utilizando *SSH* para comunicação com nós remotos, eliminando assim a necessidade de instalações de *software* adicionais nesses sistemas. Essa escolha de design não apenas simplifica o processo de implantação, mas também aumenta a segurança e reduz a sobrecarga. Além disso, a arquitetura modular do *Ansible* permite a integração de vários módulos que podem gerenciar diferentes recursos do sistema, tornando-o uma solução versátil para diversas necessidades de automação. No geral, a metodologia direta, mas eficaz, do *Ansible* facilita o gerenciamento e a orquestração eficientes em ambientes de TI complexos.

A ferramenta é caracterizada por sua simplicidade, refletida em seu processo de configuração direto e na curva de aprendizado mínima. O uso de *YAML* para a sintaxe dos *playbooks* aumenta a legibilidade e a acessibilidade, permitindo que os usuários compreendam e modifiquem facilmente os *scripts* de automação. Além disso, o *Ansible* facilita a auditoria por meio de suas capacidades de registro transparente, permitindo que os usuários rastreiem ações e mudanças de forma eficaz. Sua arquitetura sem agente reduz ainda mais a complexidade da gestão, exigindo apenas *SSH* ou *WinRM* para comunicação com os sistemas-alvo, minimizando assim a necessidade de *software* pré-instalado. Coletivamente, esses recursos contribuem para a reputação do *Ansible* como uma ferramenta poderosa, segura e amigável para automatizar processos de TI (Hochstein; Moser, 2017).

Vários termos chave são fundamentais para o entendimento da estrutura operacional do Ansible. Os ***hosts*** referem-se aos sistemas ou máquinas que são gerenciados e configurados por meio da automação. Esses *hosts* podem incluir servidores físicos, máquinas virtuais ou contêineres. Um ***playbook*** serve como o principal arquivo de configuração, que delineia uma série de tarefas a serem executadas em *hosts* especificados. O **inventário** é um componente crucial que define a coleção de *hosts* gerenciados, permitindo que os usuários organizem e direcionem grupos específicos de sistemas para automação. As ***roles*** são um mecanismo estrutural dentro do *Ansible* que facilitam a organização de *playbooks* em componentes reutilizáveis, promovendo a modularidade e escalabilidade nas práticas de automação. Além disso, **tarefas** representam ações individuais definidas dentro dos *playbooks* ou das *roles*, enquanto ***handlers*** são tarefas especiais que são acionadas por notificações de outras tarefas, permitindo uma gestão eficiente dos estados do sistema. Coletivamente, esses termos encapsulam as funcionalidades centrais do

Ansible, permitindo que os usuários implementem soluções de automação robustas e eficientes em diversos ambientes.

2.1.6 Automação de fluxos de trabalho

A automação de fluxos de trabalho e integrações entre sistemas tem se tornado uma prática fundamental em ambientes empresariais, especialmente com o aumento da complexidade das infraestruturas digitais. O conceito de automação de fluxos refere-se à capacidade de automatizar sequências de tarefas repetitivas e coordenadas entre diferentes ferramentas e serviços. Isso não apenas economiza tempo, mas também reduz a ocorrência de erros manuais, aumenta a produtividade e melhora a eficiência operacional. Em muitos casos, a automação permite que equipes de TI e negócios concentrem seus esforços em atividades mais estratégicas, ao invés de gerenciar tarefas rotineiras.

Os sistemas de integração surgem como soluções chave em ambientes onde múltiplas plataformas, sistemas e *APIs* precisam se comunicar entre si. No mundo atual, onde as empresas utilizam uma variedade de soluções especializadas (como CRMs, ERPs e ferramentas de marketing), a integração garante que os dados fluam de forma contínua e sem interrupções entre essas ferramentas. Tradicionalmente, a integração entre sistemas exigia desenvolvimentos personalizados complexos, mas com o avanço de plataformas de *iPaaS* (Plataforma de Integração como Serviço), as empresas passaram a contar com soluções que facilitam e democratizam essa conexão (Neifer *et al.*, 2021).

O *n8n* é um exemplo notável dessa nova geração de ferramentas de automação e integração. Trata-se de uma plataforma de código aberto que permite a criação de fluxos de trabalho automatizados entre diferentes serviços e *APIs* sem a necessidade de programação complexa. O diferencial do *n8n*, além de ser uma solução gratuita e acessível, é sua flexibilidade em termos de customização e controle. Usuários podem criar fluxos sofisticados com base em uma interface visual, mas também podem inserir código personalizado onde necessário, proporcionando um equilíbrio entre simplicidade e poder.

Esses avanços ilustram como a automação e a integração estão remodelando a maneira como as empresas gerenciam suas operações digitais, possibilitando um ambiente mais dinâmico e interconectado.

2.2 Trabalhos Relacionados

Nesta seção, serão explorados trabalhos que incorporam práticas ou fazem uso de ferramentas associadas à implementação de estratégias de mitigação de vulnerabilidades em sistemas operacionais, avaliação de *benchmarks* para sistemas operacionais, *hardening* de máquinas e automação. Esses estudos fornecem conhecimentos valiosos e abordagens para fortalecer a se-

gurança e a resiliência em ambientes operacionais, abrangendo desde a limitação proativa de vulnerabilidades até a implementação eficiente de *benchmarks* e práticas de *hardening*.

No trabalho conduzido por Ferreira (2021), foi realizada a implementação de controles do *framework CIS Benchmark* em um ambiente corporativo específico. O foco principal do estudo foi fortalecer a segurança dos sistemas *Unix* utilizados por uma empresa de comércio eletrônico. O relatório resultante detalha a análise minuciosa da implementação de um plano de conformidade com o *CIS Benchmark*, abordando a avaliação de não conformidades, a aplicação rigorosa das diretrizes do *framework* e a documentação do projeto. Para essa análise, a ferramenta *Cyberwatch* desempenhou um papel crucial como instrumento de análise de vulnerabilidades e conformidade com as diretrizes de segurança. Embora a ferramenta tenha demonstrado sucesso na identificação de vulnerabilidades, auxiliando assim em um plano corretivo, a comparação com outras ferramentas, como *CIS-CAT Lite* e *CIS-CAT Pro*, foi apresentada no relatório. Apesar de a ferramenta *CIS-CAT Pro* ter sido identificada como a opção mais abrangente, o estudo sugeriu o uso da *CIS CAT Lite* por ser uma versão gratuita, mantendo a capacidade de atender e superar todos os requisitos da *Cyberwatch* (Ferreira, 2021), como mostra a Tabela 2.1.

	CIS-CAT Lite	Cyberwatch	CIS-CAT Pro
Custo	Grátis	Pago	Pago
Benchmarks de sistemas operativos	ok	ok	ok
Benchmarks de Google Chrome	ok	-	ok
Outros Benchmarks	-	-	ok
Resolução automatizada de não conformidades	-	-	ok
Funcionalidade de scan de diretrizes	ok	ok	ok
Levantamento de vulnerabilidades	ok	ok	ok
Repositórios de configurações completos e íntegros	ok	-	ok

Tabela 2.1 – Comparação entre Cyberwatch e CIS-CAT

Já neste estudo de caso, Sasidharan (2022) utiliza diversos módulos fornecidos pela *CIS Security Suite*, incluindo o CIS-CAT Pro. Foram definidos metodologia, processos e etapas para a implementação dos controles de *Hardening* sugeridos pelo *CIS Benchmark* na infraestrutura composta por sistemas operacionais *Windows*. As ferramentas utilizadas vão desde o *CIS Benchmark* para guiar as práticas de segurança na configuração do sistema alvo, o *CIS Build Kit Remediation*, que oferece a aplicação automatizada de configurações recomendadas e o *CIS-CAT Pro Assessor*, para verificar, relatar e revisar a conformidade das configurações do sistema. O fluxo utilizado para testar a implementação da configuração, compreende a execução de uma avaliação do servidor *Windows* com o *CIS-CAT Pro* para obter o relatório do estado atual de conformidade do servidor. Posteriormente, o *Build Kit Remediation* é executado para implementar diversas configurações no servidor, alinhadas aos *benchmarks* CIS do sistema. Por fim, uma segunda avaliação é realizada para comparar os resultados. Como resultado dessas etapas, a pontuação final aumentou significativamente de 28,87% para 98,26% de conformidade (Sasidharan, 2022).

Por outro lado, Echeverria, Cevallos, Ortiz-Garces e Andrade (2021) propõem um modelo mais completo de Hardening, porém em um sistema de Internet das Coisas (IoT, do inglês *Internet of Things*). O modelo proposto visa reduzir riscos, ameaças e vulnerabilidades em sistemas IoT, aproveitando normas, padrões e metodologias já estabelecidas no mercado. Este trabalho destaca a aplicação de controles de *Hardening*, conforme delineado pelos *benchmarks* e diretrizes do *Center for Internet Security* (CIS), para aprimorar a postura de segurança de dispositivos IoT. Além disso, o modelo incorpora uma abordagem sistemática para o fortalecimento da segurança, incluindo etapas como definição de propósito e requisitos, modelagem de ameaças, análise de vulnerabilidades e monitoramento contínuo (Fig. 2.3). A análise dos autores destaca a importância da redução de riscos, padronização, gerenciamento de vulnerabilidades e melhoria contínua como conceitos chave no modelo proposto (Echeverría *et al.*, 2021). Embora o modelo seja projetado para sistemas IoT, pode ser adaptado para uso em outros contextos, como os ambientes *Windows*, *Linux* ou MAC, por exemplo.

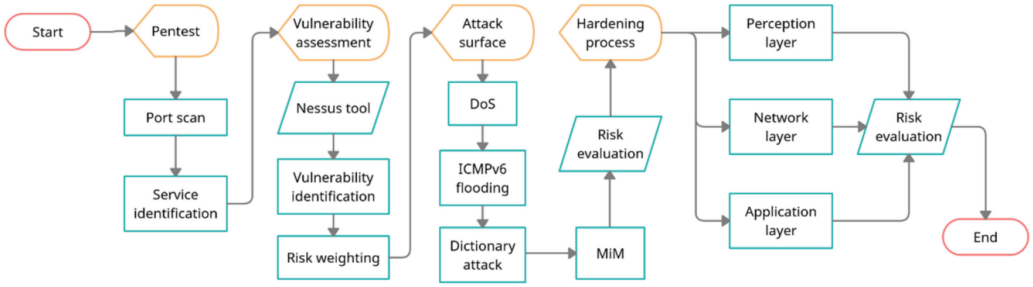

Figura 2.3 – Modelo de avaliação de risco.

3 Desenvolvimento

3.1 Framework

Limitar vulnerabilidades de um sistema não é uma tarefa simples. A escolha de um padrão de segurança prático e eficaz tem papel fundamental para o alcance do objetivo proposto. O *CIS Controls* foi adotado como principal referencial, guiando a implementação dos controles por meio do *CIS Benchmarks*. Essa escolha estratégica baseia-se na robustez e reconhecimento internacional do *Center for Internet Security* (CIS) no estabelecimento de práticas de segurança eficazes. O *CIS Controls* oferece um conjunto abrangente de diretrizes e recomendações, enquanto os *CIS Benchmarks* fornece orientações específicas para a configuração segura de sistemas.

Foi utilizado o *Benchmark* 'CIS Microsoft Windows 11 Enterprise Benchmark v2.0.0', seguindo como referência a versão 8 do *CIS Controls*. Este *Benchmark* possui 18 grupos de recomendações (Tabela 3.1), cada um abordando áreas específicas de configuração e segurança do sistema operacional. Cada grupo, por sua vez, contém diversas recomendações configuráveis, proporcionando um conjunto detalhado de diretrizes para otimizar a segurança do ambiente *Windows 11 Enterprise*. Essas recomendações estão associadas a diferentes Grupos de Implementação (IG1, IG2, IG3) do *CIS Controls*, estrutura que define a maturidade e abrangência das práticas de segurança. Além disso, cada recomendação mantém uma relação direta com um controle específico do CIS, vinculando-se a princípios fundamentais estabelecidos para proteção e mitigação de ameaças. Essa abordagem integrada e estruturada permite uma implementação abrangente e personalizada das diretrizes de segurança, alinhada aos padrões reconhecidos internacionalmente do *Center for Internet Security*.

Nessa prova de conceito, foi implementado o primeiro grupo de recomendações do *Benchmark*, focalizando nas políticas de conta. Esse grupo engloba configurações fundamentais relacionadas à segurança de senhas e ao bloqueio de contas de usuário, conforme detalhado na tabela 3.2. A escolha dessa abordagem inicial visa avaliar de maneira concreta e eficaz a viabilidade técnica da implementação dessas configurações, fornecendo entendimentos valiosos para decisões subsequentes do aprimoramento da segurança no ambiente.

3.2 Métricas

A aplicação e análise de métricas desempenham um papel crucial, oferecendo não apenas uma medida quantitativa do progresso, mas também percepções significativas para avaliação e tomada de decisões. No desenvolvimento deste trabalho, as métricas selecionadas permitem uma avaliação precisa da conformidade com os controles de segurança propostos. A escolha

	Grupo de recomendações
1	Políticas de conta
2	Políticas locais
3	Registro de eventos
4	Grupos restritos
5	Serviços do sistema
6	Registro
7	Sistema de arquivos
8	Políticas de rede com fio
9	Firewall do Windows Defender com segurança avançada
10	Políticas do gerenciador de lista de rede
11	Políticas de rede sem fio
12	Políticas de chaves públicas
13	Políticas de restrição de software
14	Configuração do cliente NAP de proteção de acesso à rede
15	Políticas de controle de aplicações
16	Políticas de segurança de IP
17	Configuração avançada de política de auditoria
18	Modelos Administrativos

Tabela 3.1 – Grupos de recomendações do CIS Microsoft Windows 11 Enterprise Benchmark v2.0.0

da ferramenta de avaliação 'CIS-CAT Lite Assessor' é fundamentada em sua eficácia como uma alternativa gratuita e abrangente, oferecendo uma análise aprofundada das configurações de segurança em conformidade com o benchmark estabelecido (Ferreira, 2021).

A avaliação do *CIS-CAT* é baseada em uma pontuação indicando a porcentagem de recomendações que já estão aplicadas no sistema alvo. Com 'RA' sendo as recomendações aplicadas e 'TR' o total de recomendações, a pontuação é definida com uma fórmula básica de porcentagem apresentada na equação 3.1. Essa pontuação pode ser calculada por grupo de recomendações ou como uma métrica global de todos os grupos contidos no *benchmark*.

$$Pontuacao(\%) = \frac{RA}{TR} * 100 \tag{3.1}$$

Além da análise quantitativa das recomendações aplicadas, também foi realizada uma avaliação detalhada do desempenho em termos de tempo de execução. Para isso, comparou-se o tempo necessário para a implementação das configurações de segurança propostas, tanto por meio de uma abordagem automatizada quanto de um processo manual. Essa análise de desempenho foi essencial para demonstrar a eficiência da automação na aplicação das recomendações de segurança, especialmente na estimativa dentro do escopo do IG1. A prova de conceito desenvolvida permitiu estimar o tempo total necessário para aplicar todas as recomendações, evidenciando ganhos potenciais de produtividade e eficiência ao adotar a automação em vez da intervenção manual, sem comprometer a conformidade com os padrões de segurança estabelecidos.

Política de Senha	Grupo de implementação
Certifique-se de que 'Aplicar histórico de senha' esteja definido como '24 ou mais senha(s)'	IG1
Certifique-se de que a 'Vida máxima da senha' esteja definida como '365 dias ou menos, mas não 0'	IG1
Certifique-se de que a 'idade mínima da senha' esteja definida como '1 ou mais dia(s)'	IG1
Certifique-se de que o 'Comprimento mínimo da senha' esteja definido como '14 ou mais caracteres'	IG1
Certifique-se de que 'A senha deve atender aos requisitos de complexidade' esteja definida como 'Ativada'	IG1
Certifique-se de que 'Relaxar limites mínimos de comprimento de senha' esteja definido como 'Ativado'	IG1
Certifique-se de que 'Armazenar senhas usando criptografia reversível' esteja definido como 'Desativado'	IG2
Política de Contas	**Grupo de implementação**
Certifique-se de que a 'Duração do bloqueio da conta' esteja definida como '15 ou mais minuto(s)'	IG2
Certifique-se de que o 'Limite de bloqueio de conta' esteja definido como '5 ou menos tentativas de entrada inválidas, mas não 0'	IG2
Certifique-se de que 'Permitir bloqueio de conta de administrador' esteja definido como 'Ativado'	IG2
Certifique-se de que 'Redefinir contador de bloqueio de conta após' esteja definido como '15 ou mais minuto(s)'	IG2

Tabela 3.2 – Controles recomendados das Políticas de Conta

Outro aspecto relevante da abordagem automatizada é sua capacidade de escalabilidade. Ao contrário do processo manual, que exige a configuração individual de cada máquina, a automação com *Ansible* permite a aplicação simultânea de múltiplas recomendações em diversas máquinas do inventário. Essa característica não apenas aumenta a eficiência operacional, como também reduz o tempo total de implementação em ambientes mais complexos, nos quais o número de sistemas a serem configurados é elevado. Assim, a automação se mostra uma solução vantajosa para a implementação em larga escala, otimizando recursos e garantindo maior consistência nas configurações de segurança.

3.3 Automação de configurações

A automação das configurações recomendadas foi realizada com a ferramenta *Ansible*. Essa escolha foi baseada em sua praticidade, facilidade de uso e principalmente por oferecer módulos específicos para a execução de comandos em sistemas *Windows*. O funcionamento do *Ansible* se dá no sentido de uma receita, descrevendo um conjunto de tarefas que devem ser executadas em ordem para atingir o objetivo final. Essas receitas são chamadas de '*Playbook*'

e são peças fundamentais para a automação com a ferramenta. Outro conceito utilizado são as chamadas 'roles', que são uma maneira de organizar e estruturar os *playbooks*, tornando o código mais modular e reutilizável. Cada *role* pode representar uma função específica, contendo uma série de tarefas isoladas e bem definidas.

Nessa prova de conceito, foi estabelecido que os grupos de recomendações são representados como *playbooks* e cada recomendação específica representa uma *role*. Por sua vez, cada *role* terá documentado em seu código a versão, controle e grupo de implementação do *CIS Controls*, assim como a referência de versão e página do *CIS Benchmarks*. Dessa forma, com uma documentação padronizada, garantimos a facilidade de manutenção para equipes e agilidade para auditar os controles implementados do *framework*. A figura 3.1 representa a estrutura de código realizada, mas, como estabelecido anteriormente, foi implementado apenas a *playbook* de Políticas de Contas.

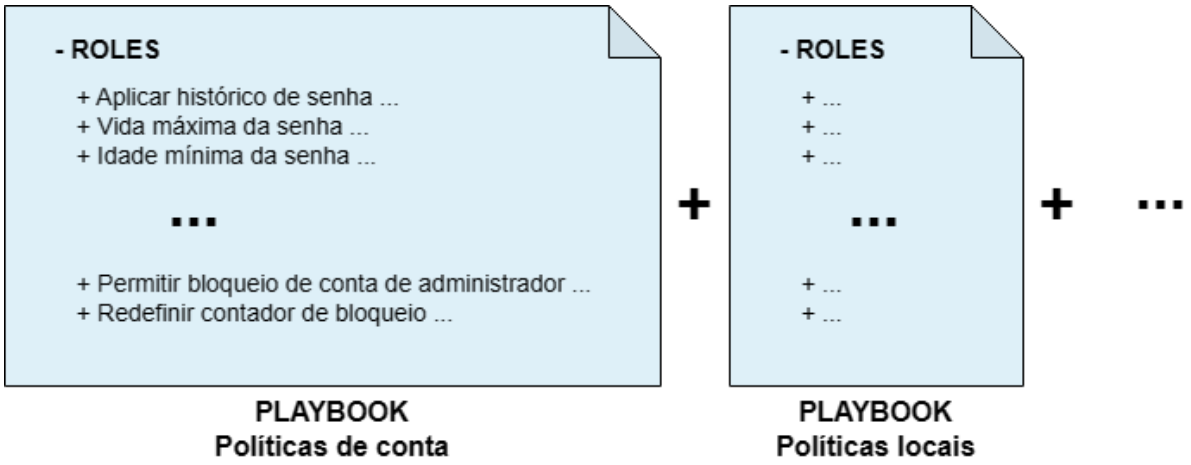

Figura 3.1 – Estrutura de código.

3.4 Fluxo de implementação

A implementação desta prova de conceito consiste em dois segmentos principais. No primeiro, as configurações foram realizadas de forma manual no sistema operacional, enquanto no segundo, utilizaram-se *scripts* automatizados para a execução das mesmas tarefas. Ambos os segmentos seguem o mesmo fluxo, sendo a única diferença a forma de realização do *Hardening* no sistema. A motivação central deste fluxo é evidenciar a eficiência e o valor das automações, demonstrando, com resultados quantitativos, como a automação supera os processos manuais em termos de tempo e consistência.

A figura 3.2 representa o fluxo completo de implementação adotado neste trabalho, que consiste em 4 passos principais:

1. Realizar a avaliação de conformidade com o *CIS-CAT Lite* nos sistemas alvo, gerando a Pontuação 1 (a) como resultado;

2. Realizar a configuração das recomendações (*Hardening*) nos sistemas alvo, sendo essa ação manual em um segmento e automatizada em outro. O tempo de execução (b) será registrado como resultado;

3. Novamente, realizar a avaliação de conformidade com o *CIS-CAT Lite* nos sistemas alvo, gerando a Pontuação 2 (c) como resultado;

4. Por fim, produzir um relatório com os resultados obtidos, comparando, em um gráfico de pontuação por tempo, ambas abordagens, manual e automatizada, assim como uma estimativa para implementações futuras de mais controles.

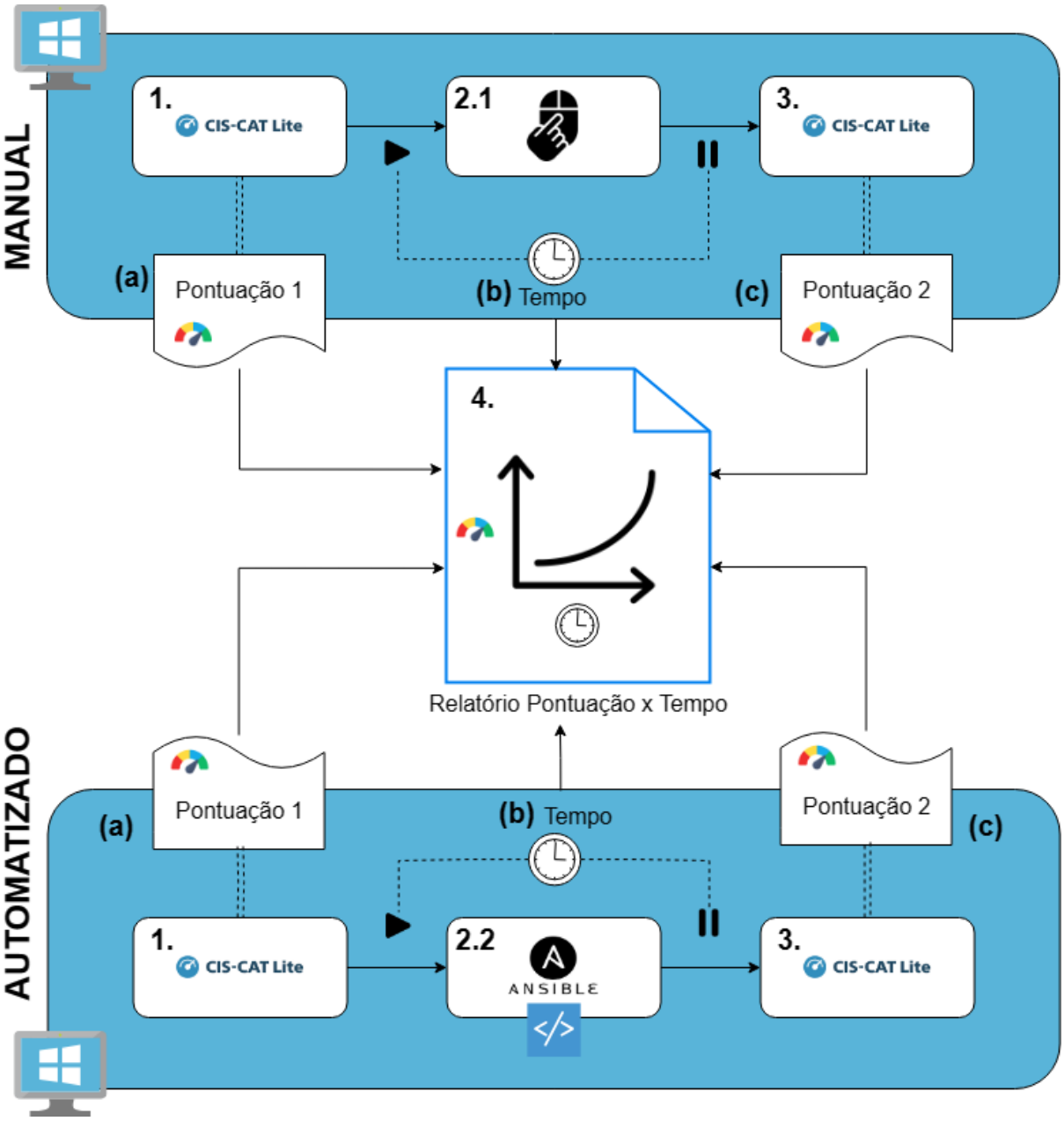

Figura 3.2 – Fluxo de implementação e metrificação.

Esse fluxo é estruturado para demonstrar, de forma prática, a eficácia da automação em comparação com métodos manuais. Ao comparar os tempos de execução e as pontuações de conformidade das duas abordagens, o fluxo evidencia como a automação pode agilizar processos, reduzir erros humanos e melhorar a padronização das configurações. É importante destacar que este fluxo de implementação não utiliza o *n8n*, pois seu objetivo principal é gerar resultados quantitativos para validar a tese de que automações são valiosas. Os fluxos do *n8n*, desenvolvidos posteriormente, têm como propósito evidenciar e sugerir formas de adaptar essas automações às realidades específicas de cada empresa, apresentando as integrações de maneira mais visual e acessível. Assim, eles servem como uma proposta prática para a implementação dessas automações, demonstrando como as empresas podem adotar e ajustar essas soluções de forma eficiente e personalizada.

3.5 Fluxos de trabalho com n8n

Neste trabalho, foram desenvolvidos diversos fluxos de exemplo com o n8n para auxiliar empresas na implementação automatizada de controles de segurança e na gestão de suas infraestruturas. Esses fluxos têm como objetivo principal automatizar o início das configurações, realizar avaliações de conformidade e executar ações subsequentes de acordo com as necessidades e processos específicos de cada organização.

Os fluxos desenvolvidos iniciam automatizando as configurações recomendadas em diversos ativos utilizando o *Ansible*, garantindo que as tarefas sejam executadas de forma padronizada e eficiente em múltiplos hosts simultaneamente. Após a aplicação das configurações, o n8n aciona o *CIS-CAT* para realizar uma avaliação detalhada das configurações de segurança, gerando uma pontuação que reflete a conformidade dos sistemas em relação aos benchmarks de segurança estabelecidos.

Com base nos resultados do *CIS-CAT*, o n8n pode realizar uma série de atividades automatizadas para apoiar os processos empresariais. Entre as possibilidades, destacam-se o envio de notificações para equipes responsáveis, a geração de relatórios detalhados sobre o tempo de execução das configurações e a pontuação obtida na avaliação de conformidade. Esses relatórios podem ser encaminhados por e-mail, armazenados em repositórios específicos ou integrados a plataformas de comunicação corporativa.

Além disso, o n8n permite salvar dados dos ativos avaliados em bancos de dados, facilitando o acompanhamento e a análise histórica das configurações e conformidades. A ferramenta também pode integrar-se com sistemas de gerenciamento de serviços de TI (*ITSM*), permitindo a criação e o encerramento automático de chamados conforme as ações realizadas e os resultados obtidos nas avaliações de segurança. Outras funcionalidades incluem o preenchimento automatizado de planilhas de controle e a execução de atividades específicas definidas conforme os fluxos de trabalho da empresa, promovendo a automação e a otimização de processos complexos.

Esses fluxos desenvolvidos com o n8n proporcionam uma solução robusta e adaptável para a automação de configurações e avaliação de conformidade, integrando diferentes etapas de um ciclo de segurança de forma centralizada e eficiente.

4 Resultados

Os resultados apresentados nessa seção abrangem o escopo definido como a prova de conceito da limitação de vulnerabilidades. Para a execução dos fluxos propostos, foram utilizadas 12 máquinas virtuais (*hosts*) com o sistema operacional *Windows 11 Enterprise* em funcionamento, todas estando em um mesmo estado inicial de configurações padrão de instalação. Como primeiro passo, foi executada a ferramenta *CIS-CAT Lite* nas 12 máquinas, com o objetivo de avaliar a conformidade de controles recomendados pelo *Benchmark* do sistema. A pontuação geral obtida foi de 22% nas instâncias, indicando que 82 dos 381 controles estavam em conformidade, sendo que 2 destes controles deveriam ser auditados manualmente, não entrando no cálculo da porcentagem de pontuação. Por outro lado, considerando apenas o grupo de recomendação das Políticas de conta, a pontuação é de 20%, indicando que duas das 11 recomendações estão aplicadas, onde uma delas não é auditada automaticamente pelo programa.

Em seguida, foram aplicadas as configurações planejadas da Política de conta, como apresentado no apêndice A.1. Durante a fase de configuração manual em uma das máquinas, cada ação correspondente a um controle específico foi cronometrada, obtendo 2 minutos e 19 segundos como tempo total de configuração dos 11 controles. Já durante o processo automatizado via *Ansible*, para apenas um *host*, a execução da *playbook* já informa o tempo de execução de cada *role*, totalizando 59 segundos para a aplicação das configurações planejadas. Em uma terceira abordagem, foram executadas, de forma automatizada, as configurações em 10 *hosts* simultaneamente, totalizando 3 minutos e 18 segundos, como apresentado no apêndice B.1. A tabela 4.1 mostra o tempo individual de cada controle, assim como a soma e a média destas medidas.

Um novo relatório de conformidade do *CIS-CAT Lite* foi executado em todas as instâncias, que novamente obtiveram o mesmo resultado de pontuação, pelo motivo de que as mesmas configurações foram aplicadas nos dois processos. Com os 11 controles do primeiro grupo de recomendação aplicados, foi obtido uma pontuação geral de 24%, resultando em uma diferença de 2% da avaliação anterior. Essa diferença não é muito expressiva devido a baixa quantidade de controles implementados nessa prova de conceito em comparação com a quantidade total de recomendações do *benchmark*, mas já indica que é possível evoluir com uma solução tanto manual quanto via *Ansible*.

Por fim, com a conclusão do fluxo e todos os resultados armazenados, foram gerados dois gráficos para análise e comparação das abordagens manual e automatizada, a fim de atestar o objetivo da prova de conceito, mensurando o possível ganho de tempo na adoção de medidas automatizadas. A figura 4.1 é uma representação fiel da pontuação por tempo de aplicação das 11 recomendações, podendo observar que a solução automatizada oferece um ganho de pontos de

Recomendação	Tempo Manual (x1)	Tempo automatizado (x1)	Tempo automatizado (x10)
Aplicar histórico de senha	0:00:16	0:00:06	0:00:16
Vida máxima da senha	0:00:15	0:00:05	0:00:17
Idade mínima da senha	0:00:15	0:00:05	0:00:16
Comprimento mínimo da senha	0:00:12	0:00:05	0:00:19
A senha deve atender aos requisitos de complexidade	0:00:10	0:00:06	0:00:16
Relaxar limites mínimos de comprimento de senha	0:00:12	0:00:05	0:00:38
Armazenar senhas usando criptografia reversível	0:00:07	0:00:06	0:00:17
Duração do bloqueio da conta	0:00:16	0:00:05	0:00:16
Limite de bloqueio de conta	0:00:13	0:00:06	0:00:14
Permitir bloqueio de conta de administrador	0:00:11	0:00:05	0:00:14
Redefinir contador de bloqueio de conta após	0:00:12	0:00:05	0:00:15
SOMA	0:02:19	0:00:59	0:03:18
MÉDIA	0:00:13	0:00:05	0:00:16

Tabela 4.1 – Tabela de tempo por configuração aplicada

forma mais ágil que manualmente. Já a figura 4.2 além de mostrar o tempo para implementação dos 11 controles, oferece também uma estimativa para a configuração dos 79 classificados como IG1, das 381 recomendações totais do *benchmark* e também da quantidade de configurações feitas com um inventário de 10 hosts, baseada na média de tempo para a configuração de cada recomendação (Tabela 4.2). Essa comparação revela uma clara disparidade entre os métodos, com a abordagem automatizada se destacando significativamente na redução do tempo de execução. Esse diferencial reforça a importância do conceito de inventário no *Ansible*, que possibilita uma escalabilidade eficaz, permitindo que as configurações sejam aplicadas simultaneamente em diversos ativos de forma ágil e padronizada. Essa capacidade de gerenciar múltiplos sistemas de maneira eficiente e escalável torna o *Ansible* uma ferramenta essencial para empresas que buscam otimizar suas operações de segurança em ambientes de infraestrutura complexos.

Número de recomendações	Tempo Manual (x1)	Tempo automatizado (x1)	Tempo automatizado (x10)
Início: 0	0:00:00	0:00:00	0:00:00
Prova de conceito : 11	0:02:19	0:00:59	0:00:18
IG1: 79	0:16:28	0:06:35	0:02:06
Prova de conceito x10: 110	0:22:55	0:09:10	0:03:18
Todas recomendações: 381	1:19:23	0:31:45	0:10:10
IG1 x10: 790	2:44:35	1:05:50	0:21:04
Todas recomendações x10: 3810	13:13:45	5:17:30	1:41:36

Tabela 4.2 – Tabela de tempo por número de configurações

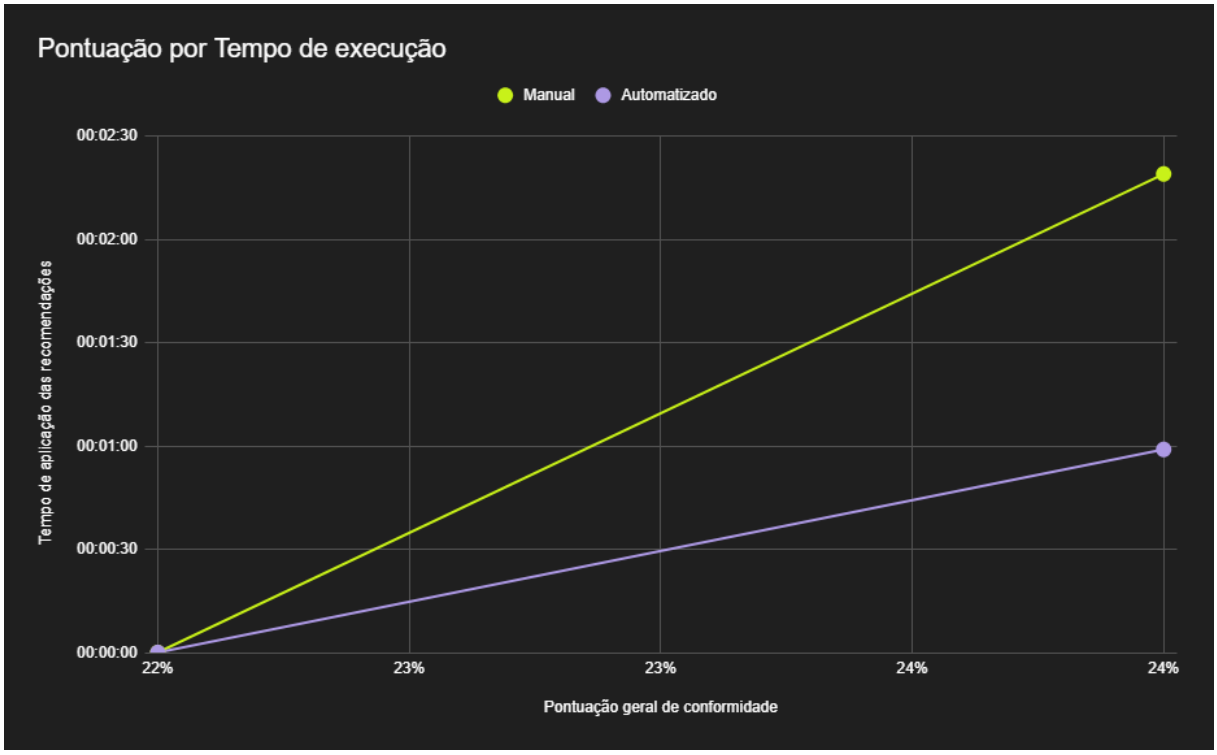

Figura 4.1 – Pontuação por Tempo de execução.

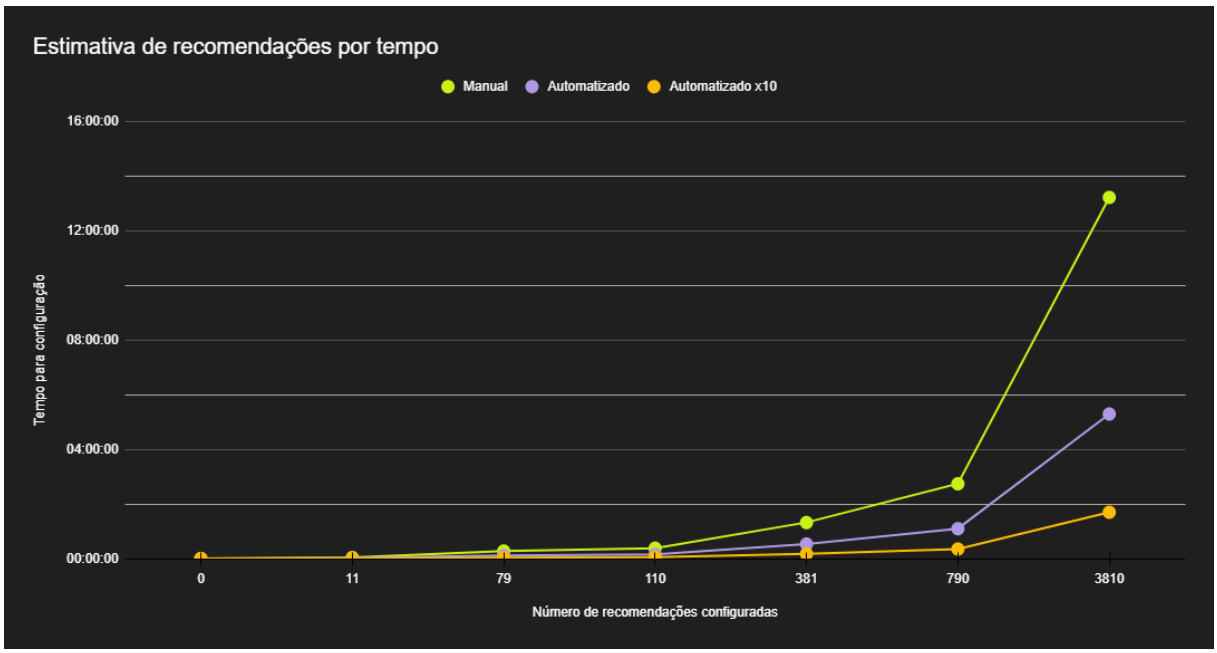

Figura 4.2 – Estimativa de recomendações por tempo.

Além dos resultados obtidos nas abordagens manual e automatizada, foram desenvolvidos fluxos de trabalho no *n8n* para exemplificar como as automações podem ser adaptadas a diferentes cenários empresariais. Esses fluxos visam não apenas a execução das configurações de segurança, mas também a integração de atividades subsequentes que variam conforme as necessidades específicas de cada organização. Com a flexibilidade do *n8n*, é possível customizar as automações

para incluir notificações, relatórios, e interações com sistemas de gerenciamento de serviços de TI, permitindo que cada empresa otimize seus processos de acordo com sua estrutura e requisitos operacionais. Essa abordagem amplia a aplicabilidade das soluções automatizadas, demonstrando como as empresas podem maximizar a eficiência na gestão de suas infraestruturas de segurança.

Os fluxos de trabalho desenvolvidos no n8n realizam todos os mesmos passos, que incluem a execução do CIS-CAT e a aplicação das configurações de segurança, mas são projetados para atender à diferentes necessidades de registro e comunicação.

1. O primeiro fluxo é acionado manualmente e, ao ser iniciado, cria uma tarefa no *Jira Software* para registrar a configuração de segurança. Após as configurações, os resultados obtidos são registrados em uma planilha do *Google Sheets*, a tarefa no *Jira* é atualizada e encerrada, e uma notificação é enviada via *Slack* para manter a equipe informada (Figura 4.3);

2. O segundo fluxo, que é executado automaticamente a cada mês, garante a conformidade e evita desconfigurações por parte dos usuários. Este fluxo realiza as configurações, registra os resultados em uma tabela do *ServiceNow*, realiza o envio de e-mails para as equipes de segurança e TI pelo *Gmail*, além de notificar via mensagem no *Discord* (Figura 4.4);

3. O terceiro fluxo, semelhante aos anteriores, registra os resultados em um banco de dados *Google BigQuery*, utiliza o *Mailgun* para enviar e-mails e notifica a equipe pelo *Microsoft Teams* (Figura 4.5);

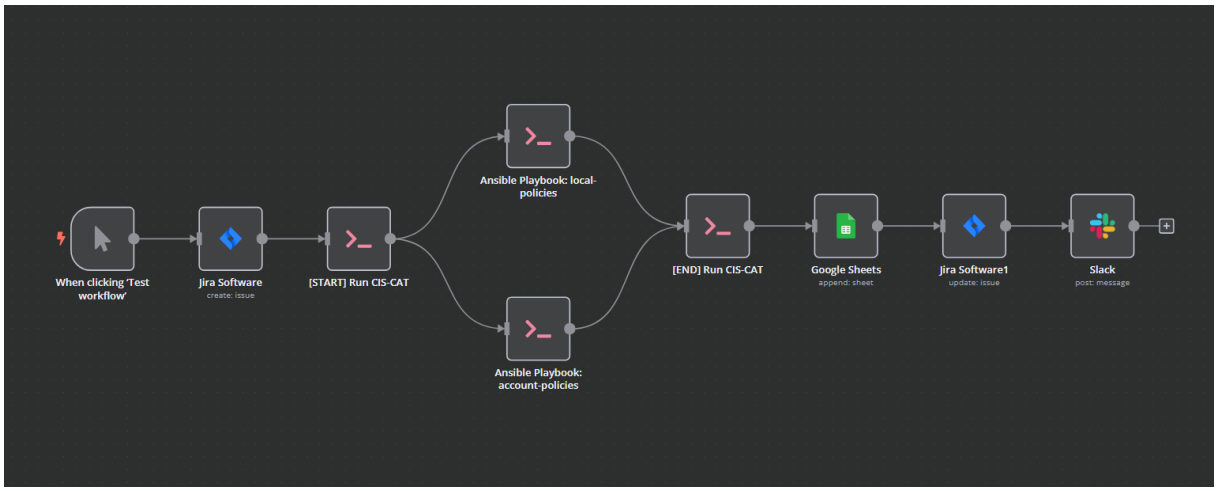

Figura 4.3 – Fluxo de trabalho com Ansible, Jira, Sheets e Slack.

Esses fluxos demonstram como o n8n pode ser utilizado para integrar diferentes ferramentas e processos, oferecendo uma abordagem robusta para a automação de configurações de segurança assim como outras tarefas que possam ser úteis para as equipes envolvidas.

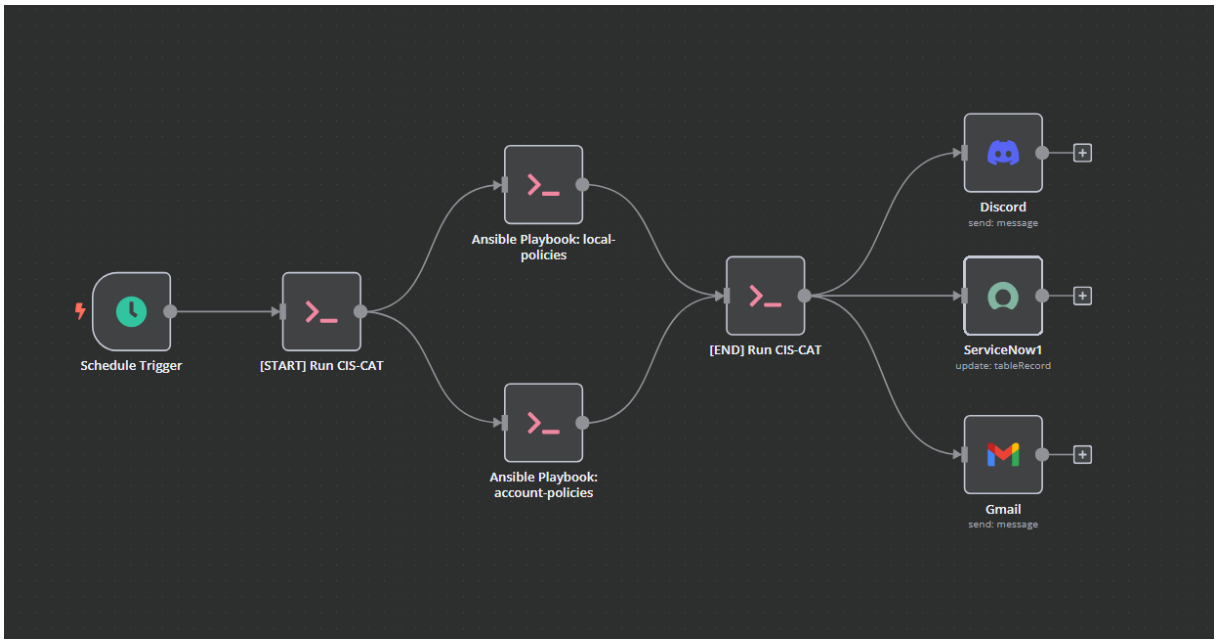

Figura 4.4 – Fluxo de trabalho com Ansible, Discord, Service Now e Gmail.

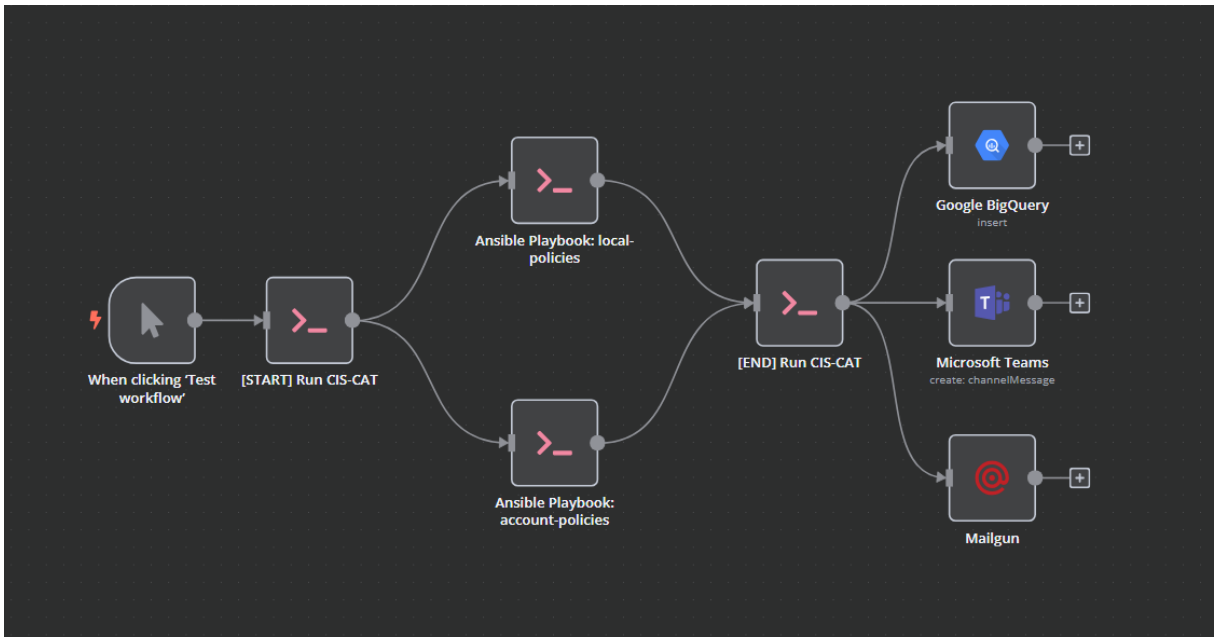

Figura 4.5 – Fluxo de trabalho com Ansible, BigQuery, Teams e Mailgun.

5 Considerações Finais

Neste trabalho foi utilizado a ferramenta *Ansible* para limitar vulnerabilidades em um sistema operacional *Windows 11 Enterprise*. Para guiar a implementação, o *CIS Benchmark* foi utilizado como *framework*, devido a sua robustez e aceitação internacional no mercado de tecnologia. Como resultado, foi comprovado em uma prova de conceito que a abordagem automatizada de configurações de segurança é de grande valia para redução do tempo operacional na implementação de tais controles, assim como foi atestado a viabilidade de codificar e avaliar um sistema sem custos adicionais de ferramenta. Esse resultado é vital para a continuação deste trabalho e tomadas de decisão sob o mesmo.

Além disso, foram desenvolvidos fluxos de trabalho na ferramenta *n8n* de código aberto, que exemplificam como as automações implementadas podem ser adaptadas e integradas aos diversos processos empresariais. Esses fluxos demonstram a capacidade de automatizar não apenas as configurações de segurança e avaliações de conformidade, mas também as atividades subsequentes, como a geração de relatórios, notificações para equipes, e o registro de resultados em diferentes plataformas corporativas. Com isso, evidencia-se que o uso de ferramentas de automação proporciona uma abordagem flexível e escalável para atender às necessidades específicas de cada organização, reforçando a tese de que as automações são cruciais para a eficiência operacional e a conformidade contínua.

5.1 Trabalhos Futuros

Esse trabalho mostra resultados promissores e abre possibilidades de melhoria e implementações mais robustas, como:

- Implementação dos 79 controles do IG1, estabelecendo a chamada "Higiene básica de segurança";
- Adição de outros tipos de testes de vulnerabilidade para avaliar o sistema, como um teste de intrusão por exemplo;

Referências

BASHOFI, I.; SALMAN, M. Cybersecurity maturity assessment design using nistcsf, cis controls v8 and iso/iec 27002. In: IEEE. **2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)**. [S.l.], 2022. p. 58–62.

CIS Benchmarks. Acessado em 22/11/2023. Disponível em: <https://www.cisecurity.org/cis-benchmarks>.

CIS Center for Internet Security. Acessado em 24/10/2023. Disponível em: <https://www.cisecurity.org/>.

CIS Controls Version 8. Acessado em 21/11/2023. Disponível em: <https://www.cisecurity.org/controls>.

CIS Critical Security Controls. Acessado em 21/11/2023. Disponível em: <https://www.cisecurity.org/controls>.

ECHEVERRÍA, A. *et al.* Cybersecurity model based on hardening for secure internet of things implementation. **Applied Sciences**, MDPI, v. 11, n. 7, p. 3260, 2021.

FERREIRA, J. P. **Hardening de Sistemas com CIS Benchmark**. Tese (Doutorado), 2021.

HOCHSTEIN, L.; MOSER, R. **Ansible: Up and Running: Automating configuration management and deployment the easy way**. [S.l.]: "O'Reilly Media, Inc.", 2017.

MCALLISTER, J. **Implementing DevOps with Ansible 2**. [S.l.]: Packt Publishing Ltd, 2017.

NEIFER, T. *et al.* Decoding ipaas: Investigation of user requirements for integration platforms as a service. In: **ICE-B**. [S.l.: s.n.], 2021. p. 47–55.

OLIVEIRA, R. S. d.; CARISSIMI, A. d. S.; TOSCANI, S. S. Sistemas operacionais. **Revista de informática teórica e aplicada. Porto Alegre. Vol. 8, n. 3 (dez. 2001), p. 7-39**, 2001.

SASIDHARAN, R. A case study to implement windows system hardening using cis controls. **International Journal of Computer Trends and Technology**, v. 70, n. 7, p. 1–7, 2022.

SHARMA, G.; KUMAR, A.; SHARMA, V. Windows operating system vulnerabilities. **International Journal of Computing and Corporate Research**, v. 1, n. 3, 2011.

SOLMS, B. V.; SOLMS, R. V. Cybersecurity and information security–what goes where? **Information & Computer Security**, Emerald Publishing Limited, v. 26, n. 1, p. 2–9, 2018.

VION, A.-L. **Software asset management and cloud computing**. Tese (Doutorado) — Université Grenoble Alpes, 2018.

Apêndices

APÊNDICE A – Scripts Ansible para Configuração do CIS Benchmark Windows

A.1 ./account-policies.yml

```
---
- hosts: win
  gather_facts: true
  roles:
  # Password Policies
  - 1.1.1-enforce-password-history
  - 1.1.2-maximum-password-age
  - 1.1.3-minimum-password-age
  - 1.1.4-minimum-password-length
  - 1.1.5-password-must-meet-complexity-requirements
  - 1.1.6-relax-minimum-password-length-limits
  - 1.1.7-store-passwords-using-reversible-encryption
  # Account Lockout Policies
  - 1.2.1-account-lockout-duration
  - 1.2.2-account-lockout-threshold
  - 1.2.3-allow-administrator-account-lockout
  - 1.2.4-reset-lockout-count
```

Listing A.1 – Playbook para Configuração de Políticas de Conta

A.2 ./roles/1.1.1-enforce-password-history/tasks/main.yml

```
---
#################################################################
#   CIS CONTROLS
#   Version:              v8
#   Control:              5 - Account Management
#   Safeguard:            5.2 - Use Unique Passwords
#   Security Function:    Protect
#   Impl Groups:          IG1
#################################################################

#################################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.1.1, page 54.
#################################################################
```

```
16
17 - name: Ensure 'Enforce password history' is set to '24 or more
       password(s)'
18   community.windows.win_security_policy:
19     section: System Access
20     key: PasswordHistorySize
21     value: 24
```

Listing A.2 – Role para controle 1.1.1 do CIS Benchmarks Windows

A.3 ./roles/1.1.2-maximum-password-age/tasks/main.yml

```
1  ---
2  ###############################################################
3  #   CIS CONTROLS
4  #   Version:              v8
5  #   Control:              5 - Account Management
6  #   Safeguard:            5.2 - Use Unique Passwords
7  #   Security Function:    Protect
8  #   Impl Groups:          IG1
9  ###############################################################
10
11 ###############################################################
12 #   CIS BENCHMARKS
13 #   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
14 #                 v1.12.0, section 1.1.2, page 57.
15 ###############################################################
16
17 - name: Ensure 'Maximum password age' is set to '365 or fewer days, but
       not 0'
18   community.windows.win_security_policy:
19     section: System Access
20     key: MaximumPasswordAge
21     value: 365
```

Listing A.3 – Role para controle 1.1.2 do CIS Benchmarks Windows

A.4 ./roles/1.1.3-minimum-password-age/tasks/main.yml

```
1  ---
2  ###############################################################
3  #   CIS CONTROLS
4  #   Version:              v8
5  #   Control:              5 - Account Management
6  #   Safeguard:            5.2 - Use Unique Passwords
```

```
#   Security Function:    Protect
#   Impl Groups:          IG1
#################################################################

#################################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.1.3, page 59.
#################################################################

- name: Ensure 'Minimum password age' is set to '1 or more day(s)'
  community.windows.win_security_policy:
    section: System Access
    key: MinimumPasswordAge
    value: 1
```

Listing A.4 – Role para controle 1.1.3 do CIS Benchmarks Windows

A.5 ./roles/1.1.4-minimum-password-length/tasks/main.yml

```
---
#################################################################
#   CIS CONTROLS
#   Version:              v8
#   Control:              5 - Account Management
#   Safeguard:            5.2 - Use Unique Passwords
#   Security Function:    Protect
#   Impl Groups:          IG1
#################################################################

#################################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.1.4, page 62.
#################################################################

- name: Ensure 'Minimum password length' is set to '14 or more
    character(s)'
  community.windows.win_security_policy:
    section: System Access
    key: MinimumPasswordLength
    value: 14
```

Listing A.5 – Role para controle 1.1.4 do CIS Benchmarks Windows

A.6 ./roles/1.1.5-password-must-meet-complexity-requirements/tasks/

```
---
############################################################
#   CIS CONTROLS
#   Version:              v8
#   Control:              5 - Account Management
#   Safeguard:            5.2 - Use Unique Passwords
#   Security Function:    Protect
#   Impl Groups:          IG1
############################################################

############################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.1.5, page 64.
############################################################

- name: Ensure 'Password must meet complexity requirements' is set to
    'Enabled'
  community.windows.win_security_policy:
    section: System Access
    key: PasswordComplexity
    value: 1
```

Listing A.6 – Role para controle 1.1.5 do CIS Benchmarks Windows

A.7 ./roles/1.1.6-relax-minimum-password-length-limits/tasks/main.y

```
---
############################################################
#   CIS CONTROLS
#   Version:              v8
#   Control:              5 - Account Management
#   Safeguard:            5.2 - Use Unique Passwords
#   Security Function:    Protect
#   Impl Groups:          IG1
############################################################

############################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.1.6, page 67.
############################################################

- name: Ensure 'Relax minimum password length limits' is set to
    'Enabled'
```

```
18   ansible.windows.win_regedit:
19     path: HKLM:\System\CurrentControlSet\Control\SAM
20     name: RelaxMinimumPasswordLengthLimits
21     data: 1
22     type: dword
```

Listing A.7 – Role para controle 1.1.6 do CIS Benchmarks Windows

A.8 ./roles/1.1.7-store-passwords-using-reversible-encryption/tasks/ma

```
1  ---
2  ###############################################################
3  #   CIS CONTROLS
4  #   Version:              v8
5  #   Control:              3 - Data Protection
6  #   Safeguard:            3.11 - Encrypt Sensitive Data at Rest
7  #   Security Function:    Protect
8  #   Impl Groups:          IG2
9  ###############################################################
10
11 ###############################################################
12 #   CIS BENCHMARKS
13 #   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
14 #                 v1.12.0, section 1.1.7, page 69.
15 ###############################################################
16
17 - name: Ensure 'Store passwords using reversible encryption' is set to
       'Disabled'
18   community.windows.win_security_policy:
19     section: System Access
20     key: ClearTextPassword
21     value: 0
```

Listing A.8 – Role para controle 1.1.7 do CIS Benchmarks Windows

A.9 ./roles/1.2.1-account-lockout-duration/tasks/main.yml

```
1  ---
2  ###############################################################
3  #   CIS CONTROLS
4  #   Version:              v8
5  #   Control:              4 - Secure Configuration of Enterprise Assets
       and Software
6  #   Safeguard:            4.10 - Enforce Automatic Device Lockout on
       Portable End-User Devices
```

```
#   Security Function:    Respond
#   Impl Groups:          IG2
#################################################################

#################################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.2.1, page 71.
#################################################################

- name: Ensure 'Account lockout duration' is set to '15 or more
    minute(s)'
  # This will only work if you
  # 1- Set the Account lockout threshold through the LockoutBadCount to
      a value greater than 0, and
  # 2- Ensure the value you are setting for LockoutDuration is greater
      than or equal to ResetLockoutCount.
  community.windows.win_security_policy:
    section: System Access
    key: LockoutDuration
    value: 15
```

Listing A.9 – Role para controle 1.2.1 do CIS Benchmarks Windows

A.10 ./roles/1.2.2-account-lockout-threshold/tasks/main.yml

```
---
#################################################################
#   CIS CONTROLS
#   Version:              v8
#   Control:              4 - Secure Configuration of Enterprise Assets
    and Software
#   Safeguard:            4.10 - Enforce Automatic Device Lockout on
    Portable End-User Devices
#   Security Function:    Respond
#   Impl Groups:          IG2
#################################################################

#################################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.2.2, page 74.
#################################################################

- name: Ensure 'Account lockout threshold' is set to '5 or fewer
    invalid logon attempt(s), but not 0'
```

```
18   community.windows.win_security_policy:
19     section: System Access
20     key: LockoutBadCount
21     value: 5
```

Listing A.10 – Role para controle 1.2.2 do CIS Benchmarks Windows

A.11 ./roles/1.2.3-allow-administrator-account-lockout/tasks/main.ym

```
1  ---
2  ############################################################
3  #   CIS CONTROLS
4  #   Version:              v8
5  #   Control:              4 - Secure Configuration of Enterprise Assets
       and Software
6  #   Safeguard:            4.10 - Enforce Automatic Device Lockout on
       Portable End-User Devices
7  #   Security Function:    Respond
8  #   Impl Groups:          IG2
9  ############################################################
10
11 ############################################################
12 #   CIS BENCHMARKS
13 #   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
14 #                 v1.12.0, section 1.2.1, page 71.
15 ############################################################
16
17 - name: Ensure 'Allow Administrator account lockout' is set to 'Enabled'
18   community.windows.win_security_policy:
19     section: System Access
20     key: AllowAdministratorLockout
21     value: 1
```

Listing A.11 – Role para controle 1.2.3 do CIS Benchmarks Windows

A.12 ./roles/1.2.4-reset-lockout-count/tasks/main.yml

```
1  ---
2  ############################################################
3  #   CIS CONTROLS
4  #   Version:              v8
5  #   Control:              4 - Secure Configuration of Enterprise Assets
       and Software
6  #   Safeguard:            4.10 - Enforce Automatic Device Lockout on
       Portable End-User Devices
```

```
#   Security Function:    Respond
#   Impl Groups:          IG2
#################################################################

#################################################################
#   CIS BENCHMARKS
#   Reference: CIS Microsoft Windows 10 Enterprise Benchmark
#                 v1.12.0, section 1.2.3, page 77.
#################################################################

- name: Ensure 'Reset account lockout counter after' is set to '15 or
    more minute(s)'
  community.windows.win_security_policy:
    section: System Access
    key: ResetLockoutCount
    value: 15
```

Listing A.12 – Role para controle 1.2.4 do CIS Benchmarks Windows

APÊNDICE B – Log de execução das configurações

B.1 Configuração de 10 máquinas simultaneamente

```
PLAY [win]
    ***************************************************************

TASK [Gathering Facts]
    ***************************************************
Sunday 29 September 2024  13:27:26 -0300 (0:00:00.020)
    0:00:00.020 ******
ok: [hardening.host0]
ok: [hardening.host1]
ok: [hardening.host2]
ok: [hardening.host3]
ok: [hardening.host4]
ok: [hardening.host5]
ok: [hardening.host6]
ok: [hardening.host8]
ok: [hardening.host7]
ok: [hardening.host9]

TASK [1.1.1-enforce-password-history : Ensure 'Enforce password
    history' is set to '24 or more password(s)']
    *******************************************************
Sunday 29 September 2024  13:27:48 -0300 (0:00:21.975)
    0:00:21.996 ******
ok: [hardening.host0]
ok: [hardening.host2]
ok: [hardening.host1]
ok: [hardening.host3]
ok: [hardening.host4]
ok: [hardening.host5]
ok: [hardening.host6]
ok: [hardening.host7]
ok: [hardening.host8]
ok: [hardening.host9]

TASK [1.1.2-maximum-password-age : Ensure 'Maximum password age' is set
    to '365 or fewer days, but not 0']
    *******************************************************
```

```
Sunday 29 September 2024  13:28:05 -0300 (0:00:16.398)
    0:00:38.394 ******
ok: [hardening.host0]
ok: [hardening.host1]
ok: [hardening.host2]
ok: [hardening.host3]
ok: [hardening.host4]
ok: [hardening.host5]
ok: [hardening.host6]
ok: [hardening.host7]
ok: [hardening.host9]
ok: [hardening.host8]

TASK [1.1.3-minimum-password-age : Ensure 'Minimum password age' is set
    to '1 or more day(s)']
    ********************************************************************
Sunday 29 September 2024  13:28:22 -0300 (0:00:17.247)
    0:00:55.641 ******
ok: [hardening.host0]
ok: [hardening.host1]
ok: [hardening.host2]
ok: [hardening.host3]
ok: [hardening.host4]
ok: [hardening.host5]
ok: [hardening.host6]
ok: [hardening.host7]
ok: [hardening.host8]
ok: [hardening.host9]

TASK [1.1.4-minimum-password-length : Ensure 'Minimum password length'
    is set to '14 or more character(s)']
    ****************************************************
Sunday 29 September 2024  13:28:38 -0300 (0:00:15.793)
    0:01:11.435 ******
ok: [hardening.host2]
ok: [hardening.host0]
ok: [hardening.host1]
ok: [hardening.host3]
ok: [hardening.host4]
ok: [hardening.host5]
ok: [hardening.host6]
ok: [hardening.host7]
ok: [hardening.host8]
ok: [hardening.host9]

TASK [1.1.5-password-must-meet-complexity-requirements : Ensure
    'Password must meet complexity requirements' is set to 'Enabled']
```

```
    **********************************
Sunday 29 September 2024  13:28:57 -0300 (0:00:19.114)
    0:01:30.549 ******
ok: [hardening.host0]
ok: [hardening.host1]
ok: [hardening.host2]
ok: [hardening.host4]
ok: [hardening.host3]
ok: [hardening.host5]
ok: [hardening.host6]
ok: [hardening.host8]
ok: [hardening.host7]
ok: [hardening.host9]

TASK [1.1.6-relax-minimum-password-length-limits : Ensure 'Relax
    minimum password length limits' is set to 'Enabled']
    ***********************************************
Sunday 29 September 2024  13:29:13 -0300 (0:00:16.255)
    0:01:46.805 ******
ok: [hardening.host1]
ok: [hardening.host3]
ok: [hardening.host2]
ok: [hardening.host4]
ok: [hardening.host0]
ok: [hardening.host9]
ok: [hardening.host5]
ok: [hardening.host7]
ok: [hardening.host6]
ok: [hardening.host8]

TASK [1.1.7-store-passwords-using-reversible-encryption : Ensure 'Store
    passwords using reversible encryption' is set to 'Disabled']
    ****************************
Sunday 29 September 2024  13:29:51 -0300 (0:00:37.876)
    0:02:24.681 ******
ok: [hardening.host2]
ok: [hardening.host4]
ok: [hardening.host0]
ok: [hardening.host1]
ok: [hardening.host3]
ok: [hardening.host5]
ok: [hardening.host6]
ok: [hardening.host7]
ok: [hardening.host8]
ok: [hardening.host9]

```

```
107 TASK [1.2.1-account-lockout-duration : Ensure 'Account lockout
    duration' is set to '15 or more minute(s)']
    ***********************************************************
108 Sunday 29 September 2024  13:30:08 -0300 (0:00:16.722)
    0:02:41.403 ******
109 ok: [hardening.host3]
110 ok: [hardening.host0]
111 ok: [hardening.host1]
112 ok: [hardening.host4]
113 ok: [hardening.host2]
114 ok: [hardening.host7]
115 ok: [hardening.host5]
116 ok: [hardening.host6]
117 ok: [hardening.host8]
118 ok: [hardening.host9]
119
120 TASK [1.2.2-account-lockout-threshold : Ensure 'Account lockout
    threshold' is set to '5 or fewer invalid logon attempt(s), but not
    0'] ****************************
121 Sunday 29 September 2024  13:30:24 -0300 (0:00:16.166)
    0:02:57.570 ******
122 ok: [hardening.host0]
123 ok: [hardening.host1]
124 ok: [hardening.host2]
125 ok: [hardening.host3]
126 ok: [hardening.host4]
127 ok: [hardening.host5]
128 ok: [hardening.host6]
129 ok: [hardening.host8]
130 ok: [hardening.host7]
131 ok: [hardening.host9]
132
133 TASK [1.2.3-allow-administrator-account-lockout : Ensure 'Allow
    Administrator account lockout' is set to 'Enabled']
    ***********************************************
134 Sunday 29 September 2024  13:30:39 -0300 (0:00:14.676)
    0:03:12.247 ******
135 ok: [hardening.host0]
136 ok: [hardening.host1]
137 ok: [hardening.host2]
138 ok: [hardening.host3]
139 ok: [hardening.host4]
140 ok: [hardening.host5]
141 ok: [hardening.host6]
142 ok: [hardening.host7]
143 ok: [hardening.host8]
144 ok: [hardening.host9]
```

```
145
146 TASK [1.2.4-reset-lockout-count : Ensure 'Reset account lockout counter
    after' is set to '15 or more minute(s)']
    ************************************************
147 Sunday 29 September 2024  13:30:53 -0300 (0:00:14.309)
    0:03:26.556 ******
148 ok: [hardening.host0]
149 ok: [hardening.host1]
150 ok: [hardening.host2]
151 ok: [hardening.host3]
152 ok: [hardening.host4]
153 ok: [hardening.host5]
154 ok: [hardening.host6]
155 ok: [hardening.host8]
156 ok: [hardening.host7]
157 ok: [hardening.host9]
158
159 PLAY RECAP
    *********************************************************************************
160 hardening.host0            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
161 hardening.host1            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
162 hardening.host2            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
163 hardening.host3            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
164 hardening.host4            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
165 hardening.host5            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
166 hardening.host6            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
167 hardening.host7            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
168 hardening.host8            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
169 hardening.host9            : ok=12   changed=0    unreachable=0
    failed=0    skipped=0    rescued=0    ignored=0
170
171 Sunday 29 September 2024  13:31:07 -0300 (0:00:14.408)
    0:03:40.964 ******
172 ===============================================================================
173 1.1.6-relax-minimum-password-length-limits : Ensure 'Relax minimum
    password length limits' is set to 'Enabled'
    ------------------------------------------- 37.88s
```

```
174 Gathering Facts
    ----------------------------------------------------------------------------
    21.98s
175 1.1.4-minimum-password-length : Ensure 'Minimum password length' is set
    to '14 or more character(s)'
    ------------------------------------------------------- 19.11s
176 1.1.2-maximum-password-age : Ensure 'Maximum password age' is set to
    '365 or fewer days, but not 0'
    ------------------------------------------------------- 17.25s
177 1.1.7-store-passwords-using-reversible-encryption : Ensure 'Store
    passwords using reversible encryption' is set to 'Disabled'
    ------------------------------ 16.72s
178 1.1.1-enforce-password-history : Ensure 'Enforce password history' is
    set to '24 or more password(s)'
    ------------------------------------------------------- 16.40s
179 1.1.5-password-must-meet-complexity-requirements : Ensure 'Password
    must meet complexity requirements' is set to 'Enabled'
    --------------------------------- 16.26s
180 1.2.1-account-lockout-duration : Ensure 'Account lockout duration' is
    set to '15 or more minute(s)'
    ------------------------------------------------------- 16.17s
181 1.1.3-minimum-password-age : Ensure 'Minimum password age' is set to '1
    or more day(s)'
    ----------------------------------------------------------------------
    15.79s
182 1.2.2-account-lockout-threshold : Ensure 'Account lockout threshold' is
    set to '5 or fewer invalid logon attempt(s), but not 0'
    ---------------------------- 14.68s
183 1.2.4-reset-lockout-count : Ensure 'Reset account lockout counter
    after' is set to '15 or more minute(s)'
    ------------------------------------------------- 14.41s
184 1.2.3-allow-administrator-account-lockout : Ensure 'Allow Administrator
    account lockout' is set to 'Enabled'
    ------------------------------------------------ 14.31s
```

Listing B.1 – Logs de execução de configuração em 10 hosts simultâneos