ESCOLA SUPERIOR DE GUERRA

JEFERSON BARBOZA MACHADO

AUTOMAÇÃO DE TAREFAS DE SEGURANÇA E MELHORIAS NA RESPOSTA A INCIDENTES CIBERNÉTICOS:

Como a automação impacta a eficácia da resposta a incidentes cibernéticos em termos de tempo e precisão?

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Cel R1 João de Azevedo

Rio de Janeiro

2024

C2024 ESG

Documento assinado digitalmente
gov.br
JEFERSON BARBOZA MACHADO
Data: 21/10/2024 13:16:09-0300
Verifique em https://validar.iti.gov.br

_____

JEFERSON BARBOZA MACHADO

RESUMO

A crescente sofisticação dos ataques cibernéticos exige respostas rápidas e precisas para garantir a segurança das organizações. Este ensaio investiga como a automação de tarefas de segurança impacta a eficácia da resposta a incidentes cibernéticos, com foco em dois aspectos críticos: tempo de resposta e precisão. O trabalho discute, ainda, as normativas brasileiras que incentivam o uso da automação e seu impacto no fortalecimento da segurança cibernética. A conclusão destaca que a automação é essencial para aumentar a resiliência das organizações diante das ameaças cibernéticas em um ambiente dinâmico e em constante transformação.

Palavras-chave: automação de segurança; resposta a incidentes; mitigação de ameaças; eficácia de resposta.

ABSTRACT

The increasing sophistication of cyber attacks requires rapid and precise responses to ensure organizational security. This essay investigates how the automation of security tasks impacts the effectiveness of cyber incident responses, focusing on two critical aspects: response time and accuracy. The work also discusses Brazilian regulations that encourage the use of automation and its impact on strengthening cybersecurity. The conclusion highlights that automation is essential for increasing organizations' resilience against cyber threats in a dynamic and constantly evolving environment.

Keywords*: security automation; incident response; threat mitigation; response effectiveness.*

1 INTRODUÇÃO

Com o avanço da transformação digital, as organizações se tornaram fortemente dependentes de sistemas de tecnologia da informação para suas operações. No entanto, essa dependência também expôs vulnerabilidades críticas que podem ser exploradas por ataques cibernéticos cada vez mais frequentes e sofisticados. A capacidade de resposta a esses incidentes se tornou crucial para a proteção dos ativos digitais e a continuidade dos negócios. Nesse contexto, a automação de tarefas de segurança cibernética surge como uma solução estratégica para mitigar riscos, aumentar a eficiência e reduzir os tempos de resposta.

A automação, aliada a ferramentas como o *Security Orchestration, Automation, and Response* (SOAR) e *Security Information and Event Management* (SIEM), permite uma resposta mais rápida e precisa a incidentes de segurança, minimizando o impacto de ataques. Esses sistemas utilizam inteligência artificial e aprendizado de máquina para automatizar processos que tradicionalmente exigiam a intervenção manual, melhorando significativamente a detecção de ameaças e a implementação de respostas. Este trabalho tem como objetivo central investigar como a automação pode impactar a eficácia da resposta a incidentes cibernéticos em termos de tempo e precisão, além de analisar as normativas brasileiras que regulamentam e incentivam o uso de tecnologias automatizadas no país.

A automação se apresenta como uma necessidade emergente, não apenas como uma ferramenta de eficiência, mas como uma defesa proativa contra ameaças cada vez mais sofisticadas. A partir dessa abordagem, o ensaio busca fornecer insights sobre as melhores práticas na implementação de soluções automatizadas para a segurança cibernética, além de destacar os desafios e oportunidades dessa estratégia no contexto organizacional brasileiro.

Para alcançar o objetivo principal deste ensaio, que é analisar como a automação impacta a eficácia da resposta a incidentes cibernéticos em termos de tempo e precisão, é necessário atingir os seguintes objetivos intermediários:

a) Analisar o papel da tríade da segurança da informação (confidencialidade, integridade e disponibilidade) na proteção dos sistemas cibernéticos: A compreensão dessa estrutura é essencial para fundamentar a importância da automação como mecanismo de defesa.

b) Explorar as ferramentas de automação mais utilizadas na resposta a incidentes cibernéticos (SOAR e SIEM): Entender como essas tecnologias funcionam e seu impacto na redução do tempo de resposta.
c) Investigar as normativas e regulamentos brasileiros, como as instruções do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que incentivam o uso da automação: Esse objetivo visa contextualizar o uso da automação no Brasil, focando em compliance e segurança.
d) Analisar os desafios da implementação da automação nas organizações, com foco na redução de erros humanos e aumento da eficiência operacional: Isso inclui a identificação de barreiras tecnológicas e organizacionais.

2 DESENVOLVIMENTO

A segurança da informação é um elemento crucial para as organizações contemporâneas, impactando diretamente a continuidade dos negócios, a confiança dos clientes e a reputação no mercado. Com a evolução tecnológica e a crescente dependência de sistemas digitais, as ameaças cibernéticas tornaram-se mais sofisticadas e frequentes, demandando abordagens robustas e eficazes para sua mitigação. Nesse contexto, a automação desponta como uma estratégia essencial para aprimorar a resposta a incidentes cibernéticos, elevando a eficiência e a precisão das ações.

Este referencial teórico aborda os principais conceitos relacionados à segurança da informação, destacando a importância estratégica da automação na melhoria da resposta a incidentes cibernéticos. Serão explorados os fundamentos da tríade da segurança da informação, a relevância de frameworks e padrões internacionais, o impacto da automação no contexto brasileiro e os aspectos normativos e legislativos que regulamentam a segurança cibernética no país.

2.1 A Tríade da Segurança da Informação

A tríade da segurança da informação, composta pelos pilares da confidencialidade, integridade e disponibilidade, é fundamental para garantir a proteção dos ativos de informação. Esses pilares formam a base da gestão de segurança da informação e estão presentes em frameworks globais, como o ISO/IEC 27001:2022 (ISO/IEC, 2022), que regulamenta as melhores práticas para a gestão da segurança da informação, incluindo o uso de automação para monitoramento contínuo e resposta a incidentes.

2.1.1 Confidencialidade

A confidencialidade refere-se à proteção das informações contra acesso não autorizado, garantindo que apenas indivíduos, entidades ou sistemas credenciados possam acessá-las. Mecanismos como controle de acesso, criptografia e autenticação são empregados para assegurar que informações sensíveis permaneçam privadas. A automação, em conjunto com mecanismos de autenticação fortes, pode detectar e bloquear tentativas de acesso indevido em tempo real.

2.1.2 Integridade

A integridade assegura que a informação se mantenha completa e inalterada, exceto por ações autorizadas. Isso significa que os dados não devem ser modificados, destruídos ou manipulados de forma não autorizada ou acidental. A automação desempenha um papel essencial na verificação contínua da integridade dos dados, utilizando sistemas que alertam imediatamente sobre alterações inesperadas nos registros.

2.1.3 Disponibilidade

A disponibilidade garante que as informações e recursos estejam acessíveis e utilizáveis quando requisitados pelos usuários autorizados. Interrupções na disponibilidade podem resultar em perda de produtividade, receita e confiança dos clientes. Medidas como redundância de sistemas, planos de recuperação de desastres e proteção contra ataques de negação de serviço (DDoS) são implementadas para manter a disponibilidade dos serviços. A automação facilita a recuperação rápida em caso de falhas, por meio da execução de scripts que reiniciam sistemas ou redirecionam o tráfego de rede.

2.2 Importância Estratégica da Segurança da Informação

No cenário atual, a segurança da informação não é apenas uma preocupação técnica, mas um componente estratégico para as organizações. A crescente dependência de tecnologias digitais para operações comerciais, comunicação e tomada de decisão significa que a segurança dos sistemas e dados está diretamente ligada ao sucesso organizacional.

Incidentes de segurança podem resultar em impactos financeiros significativos, incluindo custos de remediação, perda de receita, multas regulatórias e danos à reputação. Ademais, a conformidade com regulamentações como a Lei Geral de Proteção de Dados (LGPD), é obrigatória, e a falha em proteger dados pessoais pode levar a penalidades legais (Brasil, 2018).

A segurança da informação estratégica envolve a integração de práticas de segurança nos processos de negócios, alinhando políticas e controles com os objetivos organizacionais. Isso inclui a gestão de riscos, a formação de uma cultura de segurança entre os colaboradores e o investimento em tecnologias que apoiem a proteção contínua

dos ativos digitais. A automação, nesse contexto, atua como peça-chave para garantir respostas rápidas e precisas, reduzindo o tempo de exposição a riscos e facilitando a conformidade com normativas locais e internacionais.

2.3 Aspectos Normativos e Legislativos no Brasil

O governo brasileiro tem incentivado o uso da automação em processos de segurança cibernética por meio de normas e regulamentações. Por exemplo, a Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nº 120, de 2022, estabelece procedimentos a serem seguidos por órgãos governamentais na gestão de incidentes cibernéticos, incentivando o uso de soluções automatizadas para uma resposta rápida e eficaz a incidentes (Brasil,2022). Adicionalmente, a Instrução Normativa nº 1/2020 do GSI/PR estabelece requisitos mínimos para a segurança cibernética, incluindo o uso de ferramentas automatizadas para monitoramento e resposta a incidentes, assegurando conformidade com padrões nacionais de segurança da informação (Brasil, 2020).

2.4 Lei Geral de Proteção de Dados (LGPD)

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018a), estabelece regras sobre o tratamento de dados pessoais, inclusive no ambiente digital, visando proteger os direitos fundamentais de liberdade e privacidade. A LGPD exige que as organizações adotem medidas de segurança adequadas, incluindo soluções automatizadas para proteção de dados e resposta a incidentes que possam comprometer sua segurança. Ferramentas de automação, como o SOAR, permitem monitorar e identificar possíveis vazamentos ou acessos indevidos a dados pessoais, garantindo uma resposta rápida para mitigar possíveis danos.

2.5 Política Nacional de Segurança da Informação

O Decreto nº 9.637/2018 institui a Política Nacional de Segurança da Informação, estabelecendo diretrizes para segurança da informação, comunicações e segurança cibernética (Brasil, 2018b). O decreto enfatiza a necessidade de proteger infraestruturas críticas e promover a gestão de riscos, além de incentivar o uso de ferramentas automatizadas para aumentar a resiliência frente a ataques cibernéticos e incidentes de segurança.

A Política orienta a estruturação de respostas a incidentes cibernéticos (Art. 5º) de forma escalável e eficaz. Isso é fundamental, principalmente considerando o crescimento de ataques envolvendo exploração de vulnerabilidades e técnicas de *ransomware*. A automação permite priorizar e responder a incidentes simultâneos, tornando a organização capaz de reagir com agilidade.

2.6 Instrução Normativa GSI nº 1/2020

A Instrução Normativa define requisitos mínimos de segurança cibernética para órgãos e entidades da administração pública federal, incentivando o uso de ferramentas automatizadas para monitoramento e resposta a incidentes (Brasil, 2020a). Associada à *International Organization for Standardization* ISO/IEC 27001:2022, enfatiza a importância de relatórios pós-incidente para aprendizado contínuo. A automação pode gerar esses relatórios de forma rápida e consistente, fornecendo feedback essencial para melhorar processos internos de segurança e conformidade com regulamentações nacionais e internacionais (ISO/IEC, 2022).

2.7 Acórdão 1768/2022 do TCU

O Acórdão 1768, de 03 de agosto de 2022, do Tribunal de Contas da União (TCU) aborda questões críticas relacionadas à segurança cibernética no âmbito da administração pública. O documento destaca a necessidade de melhorar os controles de segurança cibernética e evidencia fragilidades na implementação desses controles, com foco especial na redução de intervenções manuais nos processos de resposta a incidentes, visando aumentar a eficiência e reduzir falhas.

2.8 Frameworks e Padrões Internacionais para Automação em Segurança

Diversos frameworks internacionais orientam as melhores práticas para automação em segurança da informação, fornecendo uma estrutura robusta para que as organizações gerenciem riscos de forma eficaz e proativa.

O NIST Cybersecurity Framework (CSF), desenvolvido pelo National Institute of Standards and Technology (NIST), é amplamente adotado para estruturar a gestão de riscos cibernéticos. O CSF organiza a segurança em cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar, sendo a automação uma ferramenta crítica nas funções de Detecção e Resposta. A automação permite que incidentes sejam

detectados rapidamente e que respostas a ameaças sejam precisas e ágeis, reduzindo o tempo de reação e melhorando a eficiência das ações corretivas (NIST, 2022).

O NIST SP 800-53 fornece orientações detalhadas sobre controles de segurança e processos de resposta a incidentes, muitos dos quais podem ser automatizados. Ele apresenta um catálogo de controles de segurança e privacidade voltados ao fortalecimento da proteção dos sistemas de informação. A automação é recomendada para melhorar a eficiência e a precisão dos controles de segurança.

O NIST SP 800-61, por sua vez, foca especificamente na gestão de incidentes e destaca a importância de automatizar procedimentos de contenção e mitigação para reduzir o impacto de ataques cibernéticos. A integração entre os diferentes padrões do NIST fornece uma base sólida para o desenvolvimento de estratégias automatizadas de resposta a incidentes (NIST, 2022).

Outro padrão internacional relevante é a ISO/IEC 27001:2022, que estabelece requisitos para a implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI). A norma destaca a automação como ferramenta essencial para o monitoramento contínuo, a resposta rápida a incidentes e a mitigação de riscos, promovendo uma abordagem proativa na proteção de ativos de informação. A ISO/IEC 27001 recomenda o uso de controles automatizados para garantir a integridade, confidencialidade e disponibilidade das informações (ISO/IEC, 2022).

Esses frameworks e normas, quando integrados a soluções automatizadas, capacitam as organizações a gerenciar ameaças cibernéticas de forma mais eficiente, proporcionando respostas rápidas e precisas a incidentes. A automação melhora a capacidade de reação e aumenta a resiliência das infraestruturas de TI, ao reduzir o risco de falhas humanas e aumentar a consistência dos processos de segurança.

2.9 Portaria GSI/PR nº 93/2021

A Portaria GSI/PR nº 93, de 23 de setembro de 2021, foi elaborada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) para estabelecer diretrizes de segurança cibernética no âmbito da Administração Pública Federal. Seu principal objetivo é reforçar a proteção contra ameaças cibernéticas, promovendo a padronização de terminologias e a implementação de protocolos pré-definidos para uma resposta efetiva e automatizada a incidentes de segurança (Brasil,2021).

Os resultados esperados com a aplicação das diretrizes da Portaria incluem maior agilidade na detecção e resposta a incidentes por meio de automação, facilitando

a rápida mitigação de ameaças. A padronização de protocolos e terminologias melhora a eficiência da comunicação e coordenação entre equipes de segurança e órgãos públicos. Além disso, promove o aprimoramento contínuo das estratégias de segurança cibernética para adaptação a novas ameaças (Brasil, 2021).

2.10 Decreto nº 10.748/2021

Este decreto institui a Rede Federal de Gestão de Incidentes Cibernéticos, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), com o objetivo de promover a cooperação e o compartilhamento de informações sobre ameaças e incidentes entre órgãos públicos e privados, reforçando a automação como ferramenta essencial para aumentar a resiliência das infraestruturas críticas do país (Brasil, 2021a).

2.11 Portaria Normativa GSI nº 120/2022

Esta portaria estabelece procedimentos e responsabilidades para a gestão de incidentes cibernéticos nos órgãos e entidades da administração pública federal, enfatizando o uso da automação na resposta a incidentes (Brasil, 2022). A abordagem de automação destacada pelo NIST CSF 2.0 recomenda a integração de ferramentas para análise rápida de grandes volumes de dados e identificação de padrões ou anomalias. Isso reflete a necessidade de monitoramento e análise contínua conforme recomendado pelo Plano de Gestão de Incidentes Cibernéticos (PLANGIC), aprovado pela Portaria GSI-PR nº 120/2022. A análise automatizada agiliza a identificação e extensão de incidentes, fornecendo dados confiáveis para a tomada de decisão.

2.12 Impacto da Automação na Resposta a Incidentes no Contexto Brasileiro

No Brasil, o uso de automação na segurança cibernética está em conformidade com diversas normativas e regulamentos. A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece que as organizações devem adotar medidas técnicas e administrativas para proteger dados pessoais, o que inclui o uso de soluções automatizadas.

A Política Nacional de Segurança da Informação, instituída pelo Decreto nº 9.637 de 2018, incentiva a implementação de sistemas automatizados para a proteção de infraestruturas críticas e para a gestão de riscos de segurança cibernética. Além disso, o

Decreto nº 10.748 de 2021, que estabelece a Rede Federal de Gestão de Incidentes Cibernéticos, promove a cooperação entre órgãos públicos e privados para a detecção e resposta rápida a incidentes, destacando a automação como fator crucial para aumentar a resiliência das infraestruturas críticas.

2.13 A Importância da Automação na Segurança Cibernética

A automação na segurança cibernética envolve o uso de tecnologias para executar tarefas repetitivas e complexas com intervenção humana mínima ou nula, como o monitoramento de redes, análise de logs, detecção de ameaças e resposta a incidentes.

Ela é essencial para lidar com o grande volume e a velocidade dos dados gerados em ambientes de TI modernos. Atualmente, as equipes de segurança enfrentam desafios significativos ao tentar analisar manualmente os inúmeros alertas e eventos diários.

A Instrução Normativa nº 1/2020 define a necessidade de detecção imediata e resposta rápida a incidentes (Art. 2º), reforçando o uso de ferramentas de detecção automatizada. Ferramentas como *Security Information and Event Management* (SIEM) coletam e agregam logs e eventos de diferentes fontes, permitindo correlação e análise em tempo real. A automação no SIEM facilita a detecção precoce de anomalias e a geração de alertas precisos. Já as ferramentas de *Security Orchestration, Automation, and Response* (SOAR) oferecem capacidades avançadas de orquestração e resposta automática a incidentes, essenciais para organizações que buscam aprimorar sua postura de segurança. A ISO/IEC 27001:2022 destaca a importância da automação na gestão de riscos de segurança da informação, especialmente em processos de monitoramento e resposta contínuos, proporcionando maior precisão e agilidade.

A automação também reduz erros humanos, que frequentemente ocorrem devido à fadiga, falta de conhecimento ou pressão de tempo. Sistemas automatizados seguem procedimentos predefinidos de forma consistente, minimizando a variabilidade nas respostas a incidentes e aumentando a precisão tanto na detecção de ameaças quanto na execução de ações corretivas. Além disso, a automação libera os profissionais de segurança para tarefas mais complexas e estratégicas, como análise de ameaças avançadas e planejamento de medidas de segurança. Isso se conecta ao Art. 9º da Instrução Normativa nº 1/2020, que obriga os órgãos a terem uma Política de Segurança da Informação clara e definida, na qual processos de resposta automatizados podem ser centrais.

2.14 Desafios na Implementação da Automação

Apesar dos benefícios, a implementação da automação na segurança cibernética enfrenta desafios:

- **Integração de Sistemas**: A integração de diferentes ferramentas e sistemas pode ser complexa, exigindo tempo e recursos significativos.
- **Custo**: Soluções avançadas de automação podem ser caras, especialmente para pequenas e médias empresas.
- **Falsos Positivos/Negativos**: Sistemas automatizados podem gerar falsos alertas ou falhar em detectar certas ameaças, exigindo ajustes contínuos.
- **Dependência Tecnológica**: A automação excessiva pode levar à complacência, com equipes confiando cegamente nos sistemas sem monitoramento adequado.
- **Necessidade de Especialização**: A implementação e gestão de sistemas automatizados requer profissionais qualificados, o que pode ser um desafio devido à escassez de talentos na área.

Para superar esses desafios, é fundamental que as organizações planejem cuidadosamente a implementação da automação, invistam em treinamento e adotem uma abordagem equilibrada que combine tecnologia e expertise humana.

2.15 Programas de Conscientização

Além das soluções tecnológicas, a conscientização dos colaboradores é um elemento essencial na segurança cibernética. A construção de uma cultura de segurança depende da capacitação contínua de todos os membros da organização, garantindo que compreendam seu papel na proteção dos ativos digitais e saibam como identificar e responder a potenciais ameaças.

As normativas brasileiras enfatizam a importância da conscientização como parte integrante das estratégias de segurança. O Decreto nº 9.637/2018, que institui a Política Nacional de Segurança da Informação (Brasil, 2018b), destaca a necessidade de promover a cultura de segurança nas organizações, tanto públicas quanto privadas. O Decreto nº 10.748 reforça a importância de capacitar equipes para lidar com incidentes cibernéticos e implementar práticas que minimizem erros humanos.

Nesse sentido, a Instrução Normativa nº 1/2020, emitida pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), estabelece que órgãos

públicos devem investir em programas de conscientização para melhorar a segurança cibernética. A normativa incentiva o uso de ferramentas automatizadas para monitoramento do comportamento dos usuários, facilitando a identificação de áreas vulneráveis e a personalização de treinamentos com base nas atividades dos colaboradores.

Programas eficazes de conscientização reduzem significativamente o risco de incidentes causados por erros humanos, como clicar em links de phishing ou uso inadequado de senhas. A automação pode apoiar esses programas, fornecendo ferramentas para monitorar o comportamento dos usuários em tempo real, identificar áreas de risco e adaptar treinamentos conforme as necessidades específicas de cada colaborador. Soluções automatizadas permitem que as organizações ofereçam treinamentos personalizados e focados nas fraquezas identificadas, garantindo uma resposta mais eficaz às ameaças cibernéticas.

A Portaria Normativa GSI/PR nº 120/2022 salienta que a conscientização deve ser parte do plano de resposta a incidentes de cada organização pública, reforçando que o treinamento contínuo, aliado à automação de processos, aumenta significativamente a capacidade de prevenção e mitigação de incidentes cibernéticos.

Assim, o fortalecimento da segurança cibernética vai além da tecnologia e requer o desenvolvimento de uma cultura organizacional de segurança. A combinação de programas de conscientização eficazes e automação das tarefas de monitoramento e resposta é uma estratégia robusta para mitigar riscos e proteger os ativos digitais das organizações.

2.16 Resultados Estratégicos para a Segurança e Eficiência Organizacional

Com base na LGPD (Lei nº 13.709/2018) e na Política Nacional de Segurança da Informação (Decreto nº 9.637/2018), as organizações devem buscar aprimorar sua segurança e eficiência operacional por meio de três pilares estratégicos:

1. **Aumento da Resiliência**: A LGPD exige que medidas eficazes sejam adotadas para a proteção de dados pessoais (Art. 46), e a automação de processos é fundamental para respostas rápidas a violações, garantindo conformidade e minimização de danos. A Política Nacional de Segurança da Informação complementa esse aspecto ao exigir a manutenção de operações seguras e a proteção contínua de informações críticas.

2. **Eficiência Operacional e Custo-Benefício**: A automação de processos para identificação e resposta a incidentes cibernéticos está alinhada com as estratégias de segurança para infraestruturas críticas (Decreto nº 9.573/2018), promovendo eficiência operacional. A redução do tempo de resposta e dos custos associados a ataques cibernéticos é destacada pelo DBIR 2024, que reforça a necessidade de respostas rápidas e eficazes para manter competitividade operacional.
3. **Capacitação e Melhoria da Qualidade da Resposta**: A Portaria GSI-PR nº 120/2022 sublinha a importância da capacitação constante de equipes de segurança cibernética. A automação permite que essas equipes se concentrem em atividades estratégicas e políticas, elevando a qualidade da resposta a incidentes. Além disso, esse foco na melhoria contínua segue as práticas recomendadas pela ISO/IEC 27001:2022 para fortalecer a maturidade da segurança organizacional.

Esses pilares, integrados, promovem uma abordagem robusta para fortalecer a segurança da informação e aprimorar a eficiência organizacional.

2.17 Tomada de Decisão Baseada em Dados e Aprimoramento Contínuo

A Política Nacional de Infraestruturas Críticas e a Estratégia Nacional de Segurança Cibernética (Decreto nº 10.748/2021) destacam a importância de decisões baseadas em dados e o aprimoramento contínuo para fortalecer a segurança cibernética.

A Estratégia Nacional de Segurança Cibernética enfatiza o uso de abordagens baseadas em dados para a tomada de decisão, com a adoção de ferramentas automatizadas que fornecem análises em tempo real. Isso permite que gestores respondam de maneira rápida e informada durante incidentes, além de possibilitar a avaliação constante da eficácia das estratégias de prevenção e mitigação.

O aprimoramento contínuo é reforçado pelo Decreto nº 10.748/2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos. A utilização de dados provenientes de incidentes passados para o treinamento de sistemas de machine learning contribui para o desenvolvimento de uma defesa cibernética mais robusta e adaptável a novas ameaças e cenários, promovendo assim a evolução constante das medidas de segurança.

3 CONSIDERAÇÕES FINAIS

O futuro da automação na segurança cibernética é extremamente promissor, impulsionado por avanços contínuos em inteligência artificial (IA) e aprendizado de máquina (AM). Essas tecnologias aprimoram a detecção de ameaças e a resposta a ataques desconhecidos, possibilitando que os sistemas se adaptem e aprendam com padrões e tendências, tornando-os mais eficientes. A automação inteligente, combinada com IA e AM, tem o potencial de prever ataques antes mesmo que ocorram, permitindo que as organizações adotem uma postura proativa na proteção de seus ativos digitais.

A velocidade e precisão proporcionadas pela automação melhoram a eficiência operacional, reduzindo o tempo de resposta a incidentes e minimizando o tempo de inatividade. Isso também reduz os custos associados à recuperação de incidentes, melhorando o custo-benefício.

Além disso, normativas brasileiras e internacionais, incentivam a adoção de soluções automatizadas, reforçando a importância de sistemas que garantam a segurança de dados pessoais e infraestruturas críticas. A automação, nessas normativas, é vista como ferramenta indispensável para garantir conformidade com as regulamentações e reduzir os riscos associados a falhas humanas na resposta a incidentes.

No entanto, os desafios continuam a evoluir à medida que os cibercriminosos também utilizam IA para desenvolver ataques mais sofisticados. Isso ressalta a necessidade de uma evolução constante nas estratégias de defesa cibernética, onde a colaboração entre organizações, governos e fornecedores de tecnologia, como preconizado pela Rede Federal de Gestão de Incidentes Cibernéticos do Decreto nº 10.748/2021, torna-se fundamental. O compartilhamento de informações e a cooperação entre diferentes entes contribuem para o fortalecimento da segurança cibernética em escala nacional e global.

Com a automação inteligente reduzindo a carga de trabalho das equipes de segurança, esses profissionais podem se concentrar em atividades de maior valor estratégico, como a análise de ameaças avançadas e o planejamento de segurança a longo prazo.

Por fim, o futuro da automação na segurança cibernética dependerá não só dos avanços tecnológicos, mas também da capacidade das organizações de adotar essas soluções, diretrizes e apoio de forma estratégica, mantendo o equilíbrio entre a tecnologia

e o fator humano. A preparação contínua e o investimento em automação serão essenciais para enfrentar os desafios cibernéticos emergentes e garantir a resiliência das organizações em um ambiente digital cada vez mais ameaçador.

A contribuição deste trabalho para os estudos da Escola Superior de Guerra (ESG) reside na análise aprofundada dos benefícios e desafios da automação no contexto da segurança cibernética. Ao fornecer uma visão crítica sobre a automação como estratégia de defesa cibernética, este estudo oferece subsídios importantes para o desenvolvimento de políticas e práticas que podem fortalecer a segurança nacional em um ambiente digital em constante evolução. A automação não apenas aprimora a eficiência operacional, mas também oferece uma abordagem proativa e eficaz para lidar com ameaças emergentes, tornando-se uma ferramenta indispensável para a defesa cibernética moderna.

REFERÊNCIAS

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 24 set. 2024.

BRASIL. **Decreto nº 10.748, de 16 de julho de 2021**.Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm. Acesso em: 24 set. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa nº 1, de 27 de maio de 2020**. Brasília, DF: GSI, 2020. Disponível em: https://www.gov.br/gsi/pt-br/ssic/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 24 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa nº 120, de 14 de setembro de 2022**. DF, 15 set. 2022. Disponível em: https://in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918. Acesso em: 24 set. 2024.

BRASIL. Tribunal de Contas da União. **Acórdão nº 1768 de 03 de agosto de 2022**. Brasília, DF: TCU, 2022. Disponível em: https://www.tcu.gov.br. Acesso em: 24 set. 2024.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria GSI/PR nº 93, de 23 de setembro de 2021**, DF, 24 set. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 24 set. 2024.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria Normativa GSI nº 120, de 14 de setembro de 2022**, DF, 15 set. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918. Acesso em: 24 set. 2024.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria GSI/PR nº 93, de 23 de setembro de 2021**, DF, 24 set. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 24 set. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001: 2022**: Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos. Geneve: ISO/IEC, 2022. Disponível em: https://www.iso.org. Acesso em: 24 set. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: NIST, 2022. Disponível em: https://www.nist.gov. Acesso em: 24 set. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Publicação Especial NIST SP 800-53**: Controles de Segurança e Privacidade para Sistemas e Organizações de Informação. Gaithersburg: NIST, 2022. Disponível em: https://www.nist.gov. Acesso em: 24 set. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Publicação Especial NIST SP 800-61**: Gerenciamento de Incidentes de Segurança de Computador. Gaithersburg: NIST, 2022. Disponível em: https://www.nist.gov. Acesso em: 24 set. 2024.