ESCOLA SUPERIOR DE GUERRA

RENATO CÉZAR DE MOURA

AS REDES SEGREGADAS DE TI PARA O DESENVOLVIMENTO DE PROJETOS ESTRATÉGICOS DE ENGENHARIA:

os desafios para atualização e evolução dos seus ativos e a manutenção da proteção cibernética

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. R/1 João de Azevedo

Rio de Janeiro

2024

C2024 ESG

Este trabalho, nos termos de legislação que resguarda os direitos autorais, é considerado propriedade da ESCOLA SUPERIOR DE GUERRA (ESG). É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que sem propósitos comerciais e que seja feita a referência bibliográfica completa.

Os conceitos expressos neste trabalho são de responsabilidade do autor e não expressam qualquer orientação institucional da ESG.

RENATO CÉZAR DE MOURA

Documento assinado digitalmente
RENATO CEZAR DE MOURA
Data: 16/10/2024 10:04:07-0300
Verifique em https://validar.iti.gov.br

RESUMO

As redes segregadas de Tecnologia da Informação (TI) são fundamentais em ambientes computacionais que necessitam de elevado nível de segurança e eficiência, como por exemplo, para o desenvolvimento de projetos estratégicos de engenharia, onde são produzidos, inseridos, processados, armazenados e transmitidos documentos e informações digitais em grande escala e de alta sensibilidade e que, que, se divulgados ou acessados indevidamente, podem causar danos significativos à organização ou aos indivíduos envolvidos. Essas informações exigem medidas rigorosas de proteção para garantir sua confidencialidade, integridade e disponibilidade. A implementação de medidas de segurança cibernética, como firewalls, criptografia, sistemas de detecção de intrusão, monitoramento ativo da rede, testes de vulnerabilidade das aplicações e sistemas, controle de acesso físico aos dispositivos, gerenciamento e monitoramento dos acessos as informações e rotinas de salvaguarda e recuperação de dados são essenciais para proteger as informações sensíveis contra ataques e para recuperação de incidentes cibernéticos, sendo um aspecto crítico na gestão de projetos, especialmente em áreas estratégicas, onde a implementação de práticas robustas de segurança é fundamental para mitigar riscos e garantir a integridade dos dados. No entanto, a atualização e evolução dos ativos de TI em redes segregadas apresentam diversos desafios, principalmente em relação a atualização da infraestrutura, que inclui a atualização de *hardware* e *software*, que pode ser complexa e custosa, e a evolução tecnológica, que exige das redes segregadas uma complexa adaptabilidade e escalabilidade por requerer um planejamento estratégico aprimorado e investimentos contínuos, e que impactam diretamente no seu grau de proteção cibernética, tornando a manutenção da segurança cibernética deste tipo de ambiente um desafio constante. Dessa forma, foram realizadas pesquisas em livros, artigos científicos, trabalhos acadêmicos e documentos governamentais e não-governamentais buscando entender a complexidade e os desafios que a adoção de redes segregadas de TI implicam e como uma abordagem estratégica e integrada pode garantir que este tipo de solução tecnológica suporte os objetivos e atenda às necessidades do projeto estratégico, além de proteger os ativos da organização.

Palavras-chave: redes segregadas; projetos estratégicos; proteção cibernética.

ABSTRACT

Segregated Information Technology (IT) networks are essential in computing environments that require a high level of security and efficiency, such as for the development of strategic engineering projects, where large-scale and highly sensitive digital documents and information are produced, inserted, processed, stored and transmitted and, if disclosed or accessed improperly, could cause significant damage to the organization or individuals involved. This information requires rigorous protection measures to ensure its confidentiality, integrity and availability. The implementation of cybersecurity measures, such as firewalls, encryption, intrusion detection systems, active network monitoring, vulnerability testing of applications and systems, physical access control to devices, management and monitoring of access to information and data backup and recovery routines are essential to protect sensitive information against attacks and to recover from cyber incidents, and are a critical aspect in project management, especially in strategic areas, where the implementation of robust security practices is essential to mitigate risks and ensure data integrity. However, the updating and evolution of IT assets in segregated networks presents several challenges, mainly in relation to the updating of infrastructure, which includes the updating of hardware and software, which can be complex and costly, and technological evolution, which requires complex adaptability and scalability from segregated networks, as it requires improved strategic planning and continuous investments, and which directly impacts their level of cyber protection, making maintaining cyber security in this type of environment a constant challenge. Therefore, research was carried out in books, scientific articles, academic papers and governmental and non-governmental documents, seeking to understand the complexity and challenges that the adoption of segregated IT networks implies and how a strategic and integrated approach can ensure that this type of technological solution supports the objectives and meets the needs of the strategic project, in addition to protecting the organization's assets.

Keywords: *segregated networks; strategic projects; cybernetic protection.*

1 INTRODUÇÃO

As redes segregadas de Tecnologia da Informação (TI) são fundamentais no desenvolvimento de projetos estratégicos de engenharia, pois, ao serem isoladas de redes corporativas e da internet, proporcionam um ambiente seguro para a inovação e execução de tarefas complexas. No entanto, sua manutenção e atualização trazem desafios significativos, especialmente no que se refere à proteção cibernética, exigindo abordagens estratégicas bem estruturadas para garantir a segurança e a evolução contínua dessas infraestruturas.

Este estudo examina os principais desafios enfrentados por organizações na gestão de redes segregadas de TI, focando na identificação de problemas relacionados à sua adoção em projetos estratégicos de engenharia. Além disso, busca entender como diferentes entidades elaboram estratégias para gerenciar esses ambientes e garantir a cibersegurança enquanto evoluem seus ativos. A pesquisa também propõe melhores práticas para enfrentar esses desafios de forma eficaz.

A questão central deste trabalho é investigar como as restrições às redes segregadas de TI, especialmente em termos de atualização e evolução dos ativos tecnológicos, podem ser superadas para garantir a segurança cibernética necessária. A relevância do estudo é evidenciada pela aplicação dessas redes em projetos estratégicos das Forças Armadas Brasileiras, como o Projeto do Submarino Nuclear Convencionalmente Armado (SNCA), parte do Programa de Obtenção de Submarinos (PROSUB).

Com base em uma abordagem técnica sólida, este estudo visa fornecer percepções que possam orientar futuras decisões estratégicas sobre a gestão de ambientes computacionais segregados em projetos de engenharia, com foco na proteção dos ativos da organização e na manutenção da segurança cibernética.

2 DESENVOLVIMENTO

Para o desenvolvimento adequado deste trabalho, é imprescindível apresentar as definições dos principais termos abordados: projetos estratégicos de engenharia, redes segregadas de TI e segurança cibernética. Com as definições e conceitos adequadamente elucidados, este trabalho abordará a implementação das redes segregadas de TI em projetos estratégicos de engenharia, discutirá os desafios relacionados à atualização e evolução dos ativos dessas redes e examinará práticas

técnico-conceituais voltadas à manutenção da segurança cibernética das redes segregadas de TI.

2.1 Projetos Estratégicos de Engenharia

Uma definição sintética e assertiva de projeto é aquela apresentada por Grey e Larson (2016), que é um empreendimento temporário que visa criar um produto, serviço ou resultado único, com meta principal de satisfazer a necessidade do cliente, tendo as seguintes característica principais características:

a. Um objetivo estabelecido.
b. Um ciclo de vida definido, com início e fim.
c. Geralmente, envolve diversos departamentos e profissionais.
d. Comumente, faz algo que nunca foi feito antes.
e. Requisitos específicos de tempo, custo e desempenho.

Ainda segundo Grey e Larson (2016), os termos “programa” e “projeto” são frequentemente usados de forma intercambiável, o que pode causar confusão. Ambos são direcionados a objetivos específicos e requerem planos e recursos, utilizando ferramentas, métodos e políticas semelhantes. No entanto, a principal diferença está no escopo e no horizonte de tempo, sendo que:

a. Programa: Consiste em uma série de projetos múltiplos, relacionados e coordenados, que continuam por um período prolongado até atingir um objetivo comum. Exemplos de programa são o Programa de Obtenção de Submarinos (PROSUB) e o Programa Nuclear da Marinha (PNM), conduzidos pela MB (Brasil, 2020b).
b. Projeto: Cada projeto dentro de um programa tem um gerente de projetos, sendo diferença principal entre um programa e um projeto a sua escala e o seu período de tempo. Exemplos de projetos no âmbito do PROSUB e PNM são o Projeto do Ciclo de Combustível Nuclear, o Projeto da Planta Nuclear Embarcada (PNE) e o Projeto do Submarino Nuclear Convencionalmente Armado (SNCA) (Brasil, 2020a).

Um projeto de engenharia, que pode ser parte de um programa, consiste em processos e atividades planejadas para alcançar objetivos específicos, como a construção de obras, desenvolvimento de produtos ou implementação de sistemas,

sempre dentro de prazos e orçamentos definidos para atender às necessidades do cliente. Neste estudo, a definição de projetos estratégicos de engenharia segue as diretrizes da Estratégia Nacional de Defesa (END) do Brasil, um documento que orienta a capacitação das Forças Armadas para garantir a segurança do país em tempos de paz e crise. Lançada em 2008 e revisada em 2012 e 2016, a END foi atualizada em 2020, e esta versão recente é a referência utilizada neste trabalho.

A END tem como objetivos principais (Brasil, 2020b):

a. Organização das Forças Armadas: Define como as Forças Armadas devem se estruturar e operar para cumprir suas atribuições constitucionais e garantir a defesa do país.
b. Reorganização da Base Industrial de Defesa: Visa assegurar que as necessidades de equipamento das Forças Armadas sejam atendidas com tecnologias sob domínio nacional, preferencialmente de uso dual (militar e civil).
c. Composição dos Efetivos: Estabelece diretrizes sobre o efetivo das Forças Armadas e o futuro do Serviço Militar Obrigatório, garantindo que as Forças sejam formadas por cidadãos de todas as classes sociais.
d. Modernização e Desenvolvimento: Enfatiza a necessidade de modernizar a estrutura de defesa nacional e promover o desenvolvimento de setores estratégicos como o espacial, o cibernético e o nuclear.

A END também aborda questões político-institucionais, estipulando ações estratégicas de médio e longo prazo para a modernização da defesa nacional e a integração entre governo e sociedade na “grande estratégia” de segurança da nação (Brasil, 2024b).

A END é estruturada de forma a garantir uma abordagem abrangente e integrada para a defesa nacional. É importante destacar que os programas e projetos estratégicos no âmbito da defesa nacional são componentes dos setores estratégicos da END. Esses setores são definidos da seguinte maneira (Brasil, 2020b):

a. Setor Espacial: Envolve o desenvolvimento de capacidades espaciais para garantir a soberania e segurança do país, atribuído a Força Aérea Brasileira (FAB) em conjunto com a Agência Espacial Brasileira (AEB).
b. Setor Cibernético: Foca na proteção das infraestruturas críticas e na defesa contra ameaças cibernéticas, atribuído ao Exército Brasileiro (EB).

c. Setor Nuclear: Visa o desenvolvimento e a manutenção de capacidades nucleares para fins pacíficos e de defesa, atribuído a MB.

O Brasil tem se destacado na causa da não proliferação de armas nucleares, utilizando a tecnologia nuclear exclusivamente para fins pacíficos, conforme estabelecido na Constituição e no Tratado de Não Proliferação de Armas Nucleares (Brasil, 2020b). O país busca desenvolver e nacionalizar o ciclo completo do combustível nuclear, incluindo o enriquecimento e a construção de reatores, com foco no projeto do Submarino Nuclear Convencionalmente Armado (SNCA), parte do Programa de Obtenção de Submarinos (PROSUB) (Brasil, 2020a).

Projetos estratégicos de engenharia na área de defesa, como o SNCA, são fundamentais para promover o desenvolvimento científico e tecnológico, qualificar o capital humano e fortalecer a Base Industrial de Defesa (BID). Além de contribuir para a criação de produtos de uso dual (civil e militar), esses projetos geram empregos e renda, envolvendo grande interação entre os setores científico, tecnológico, econômico e industrial, com elevado impacto na segurança e soberania nacionais (Brasil, 2020b; Brasil, 2024a).

2.2 Redes Segregadas de TI

Tanenbaum, Feamster e Wetherall (2021) definem redes de computadores como sistemas que permitem a comunicação e troca de dados entre dispositivos conectados, como computadores, impressoras e roteadores, utilizando diversas configurações e tecnologias. Essas redes são essenciais para a troca de informações e o acesso a recursos. Já o termo "ambiente computacional", segundo Tanenbaum e Austin (2013), refere-se a um conjunto mais amplo de recursos e serviços que proporcionam uma plataforma para a execução de programas e gerenciamento de dados, englobando hardware, software e usuários.

Conforme as definições de Tanenbaum, Feamster e Wetherall (2021) e Tanenbaum e Austin (2013), o ambiente computacional é uma noção mais ampla que abrange a execução de tarefas e o uso de software e hardware, enquanto as redes de computadores se concentram na conectividade e comunicação entre dispositivos. Ambos são essenciais para o funcionamento eficaz de sistemas modernos, com uma ênfase no compartilhamento de recursos, tanto de software e hardware quanto de dados entre usuários e dispositivos. Para este trabalho, o termo "redes de computadores" será utilizado como sinônimo de ambiente computacional.

Abordando o termo segregação de redes de computadores, traz-se aqui a definição adotada pela MB para este termo que apresenta os conceitos de “segregação física” e a “segregação lógica” para redes de computadores, sendo (Brasil, 2019):

a. Rede Segregada Fisicamente: Trata-se de uma rede com um perímetro de segurança física definido, onde nenhuma informação pode sair por qualquer meio, incluindo dispositivos de armazenamento como USB, CD e DVD. Essa rede não pode ser conectada a outras redes e não deve ter acesso remoto; apenas indivíduos presentes fisicamente dentro do perímetro podem acessar as informações geradas, armazenadas ou processadas.
b. Rede Segregada Logicamente: Essa rede utiliza mecanismos computacionais para garantir a segurança e o controle da informação em todas as fases, como processamento, armazenamento e transmissão. Ela pode incorporar técnicas como virtualização de estações de trabalho, gerenciadores de segurança centralizados, criptografia de arquivos e ferramentas para controlar a transferência de dados via unidades USB, impressoras e e-mail, além de ter uma arquitetura de rede segura.

As redes segregadas de TI são uma estratégia crucial adotada por organizações para otimizar segurança, eficiência e conformidade (Stallings, 2020). A segregação refere-se à prática de dividir redes de computadores em segmentos ou infraestruturas distintos, de forma a limitar o acesso a informações sensíveis e a melhorar o desempenho da rede (NIST, 2020), podendo ser implementadas fisicamente, com o uso de hardware separado, ou logicamente, através de configurações de software que definem diferentes zonas de acesso (Zwicky *et al*., 2000). Essa prática é comum em diversos setores, como financeiro, saúde e tecnologia (Liu; Chen, 2018). Dentre os diferentes tipos de redes segregadas, pode-se citar:

a. Redes de Produção e Teste: mantêm ambientes separados para operações reais e experimentais, minimizando riscos de falhas (Stallings, 2020).
b. Redes Internas e Externas: separam usuários internos de visitantes para proteger dados sensíveis (Zwicky *et al*., 2000).

c. Redes de Controle de Acesso: implementam controles rigorosos para dados críticos, garantindo que apenas usuários autorizados possam acessá-los (NIST, 2020).

A adoção de redes segregadas de TI é uma prática essencial para garantir a segurança e a eficiência em um ambiente digital em constante evolução, podendo-se citar as suas seguintes vantagens:

a. Segurança Aprimorada: A segregação limita o acesso a informações sensíveis, reduzindo o risco de vazamentos de dados (SANS Institute, 2019).
b. Desempenho Eficiente: Reduz o tráfego de rede e melhora a performance ao isolar atividades (Liu; Chen, 2018).
c. Conformidade Regulatória: Facilita a adesão a normas de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) (ISO, 2022).

Cabe destacar, porém, que a implementação de redes segregadas também apresenta desvantagens, podendo ser citadas as principais:

a. Complexidade na Gestão: Gerenciar múltiplas redes pode exigir mais recursos e expertise técnica (Fowler, 2018).
b. Custo Adicional: A implementação de redes segregadas pode ser dispendiosa em termos de hardware e software (Stallings, 2020).
c. Interoperabilidade Limitada: A comunicação entre redes pode ser complexa, exigindo soluções adicionais para integração (Liu; Chen, 2018).

Haja vista que este trabalho está utilizando como referência o projeto estratégico de engenharia do SNCA, sob condução da MB, será considerada para este trabalho a definição adotada pela Força Naval brasileira.

2.3 Segurança Cibernética

A segurança cibernética tem suas raízes na cibernética, conforme definido por Wiener (1968) como o estudo da comunicação e controle em sistemas complexos, abrangendo a teoria da informação, feedback e autorregulação. Este campo visa entender como os sistemas operam, se adaptam e se auto-organizam, enfatizando as

interações entre seus componentes e o ambiente. Para este trabalho, o conceito de cibernética será aplicado principalmente nas áreas de engenharia e ciência da computação, especialmente no contexto de um projeto estratégico de engenharia de estado.

No âmbito da legislação brasileira, a definição de segurança cibernética evoluiu ao longo do tempo. Inicialmente um componente da Política Nacional de Segurança da Informação (Brasil, 2018a), tornou-se uma entidade própria com a criação da Política Nacional de Cibersegurança (Brasil, 2023). O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) é o responsável por coordenar essa área e apresenta conceitos fundamentais relacionados à cibernética que são essenciais para a compreensão do tema (Brasil, 2021), sendo:

a. Cibernética: termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e suas interações, sendo que no campo da Defesa Nacional, inclui os recursos de Tecnologia da Informação e Comunicações (TIC) de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais.
b. Espaço Cibernético: espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação, englobando todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente.
c. Segurança Cibernética: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.
d. Defesa Cibernética: ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação

de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente.

O ambiente cibernético, ou seja, os usuários, redes, dispositivos, software, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores (Brasil, 2021), está sujeito a ameaças, que pode ser entendido como o conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização (Brasil, 2021). Neste contexto, surge então o conceito de ameaça cibernética, que pode ser definida como qualquer circunstância ou evento com o potencial de causar dano a um sistema de informação através de uma exploração de vulnerabilidades, além de roubo ou alteração de dados de forma não autorizada, sendo enfatizada a intenção maliciosa e o impacto potencial sobre a segurança dos sistemas (NIST, 2012b).

As ameaças cibernéticas manifestam-se de diversas formas, sendo possível destacar algumas das mais comuns (Brasil, 2021):

a. *Malware*: *software* malicioso projetado para causar danos ou comprometer sistemas, incluem os vírus, *worms*, *botnets*, *trojans*, *spywares*, *adwares* e *rootkits*.
b. *Phishing*: técnica de enganar usuários para que revelem informações confidenciais, como senhas, geralmente por meio de e-mails fraudulentos.
c. *Ransomware*: Tipo de *malware* que criptografa dados e exige um pagamento para a recuperação dos mesmos.
d. Ataques de *Distributed Denial of Service* (DDoS): tentativas de indisponibilizar um serviço ao sobrecarregar um sistema com tráfego excessivo.
e. *Exploits*: ataques que utilizam vulnerabilidades conhecidas em software ou hardware para ganhar acesso não autorizado a sistemas.
f. Injeção SQL: técnica em que um invasor insere código SQL malicioso em um campo de entrada para manipular bancos de dados.
g. *Spoofing*: falsificação de identidade em comunicações de rede, como e-mails ou endereços *Internet Protocol* (IP), para enganar o destinatário.
h. *Advanced Persistent Threats* (APT): ataques sofisticados e de longo prazo, onde criminosos se infiltram em redes e permanecem ocultos por longos períodos.

As medidas de proteção cibernética são tão diversas quanto as ameaças que se apresentam no ambiente cibernético. Dentre essas medidas, destacam-se as principais estratégias e ferramentas utilizadas para mitigar riscos e garantir a segurança das informações:

a. *Firewalls*: dispositivos ou softwares que monitoram e controlam o tráfego de rede, bloqueando acessos não autorizados (NIST, 2009).
b. Antivírus e Antimalware: programas que detectam, previnem e removem softwares maliciosos de sistemas e dispositivos (CISA, 2020).
c. Sistemas de Detecção e Prevenção de Intrusões (IDS e IPS): ferramentas que monitoram atividades de rede em busca de comportamento malicioso e tomam medidas para bloquear esses ataques (NIST, 2007).
d. Criptografia: processo de codificação de dados para protegê-los contra acesso não autorizado, garantindo a confidencialidade e integridade das informações (NIST, 2001).
e. Autenticação Multifator (MFA): camada adicional de segurança que exige mais de uma forma de verificação para acesso a sistemas e dados (NIST, 2017b).
f. Salvaguarda (*Backup*) e Recuperação de Dados (*Restore*): estruturas e práticas para garantir que os dados possam ser recuperados em caso de perda ou ataque, como *ransomware* (NIST, 2010).
g. Educação e Conscientização de Segurança: programas de treinamento para funcionários sobre boas práticas de segurança e identificação de ameaças, como *phishing* (NIST, 2024a).

A atualização e evolução dos ativos em um ambiente cibernético são tão importantes quanto a implementação de medidas de proteção cibernética, sendo que, para garantir um elevado nível de segurança, é fundamental acompanhar as mudanças no cenário de ameaças, uma vez que novas vulnerabilidades em sistemas, softwares e hardwares surgem continuamente (NIST, 2024b). A capacidade de adaptação rápida a essas novas ameaças e vulnerabilidades é crucial para a resiliência organizacional, pois um ambiente cibernético em constante evolução se torna menos suscetível a ataques bem-sucedidos (ISO, 2022).

Portanto, a adoção de práticas regulares de atualização e a integração de novas tecnologias de segurança são essenciais para fortalecer a defesa contra riscos potenciais, sendo este assunto abordado com maior profundidade neste trabalho.

2.4 As Redes Segregadas de TI em Projetos Estratégicos de Engenharia

A crescente digitalização e interconexão de sistemas em projetos de engenharia tornam a proteção cibernética essencial, uma vez que a dependência de tecnologias digitais e automação expõe as organizações a vulnerabilidades que podem comprometer a integridade, confidencialidade e disponibilidade de informações críticas (Davis; Reiter, 2020). Setores como energia, transporte e construção lidam com dados sensíveis e infraestrutura crítica, mas a situação é ainda mais delicada no contexto da defesa, onde projetos frequentemente envolvem informações e tecnologias sigilosas relacionadas ao desenvolvimento estratégico, à soberania e à segurança nacional (Chapple, 2021).

As ameaças cibernéticas são um dos principais desafios enfrentados por organizações que trabalham em projetos de engenharia, especialmente em setores críticos e estratégicos. Entre as ameaças mais relevantes, destacam-se:

a. *Ransomware*: Esses ataques, cada vez mais sofisticados e frequentes, envolvem a criptografia de dados essenciais, tornando-os inacessíveis. Os atacantes geralmente exigem resgates pela chave de decriptação, resultando em perdas financeiras significativas e interrupções operacionais prolongadas, o que pode afetar a reputação da organização e a confiança dos clientes (Davis; Reiter, 2020). Em projetos de engenharia, essa paralisação pode causar atrasos e custos adicionais, comprometendo a entrega de serviços e produtos.

b. Espionagem: Este tipo de ataque visa a propriedade intelectual e informações estratégicas, representando uma ameaça significativa para empresas que desenvolvem tecnologias inovadoras. A perda de dados valiosos, como designs de produtos e processos de fabricação, pode levar a desvantagens competitivas e inviabilidade de projetos, além de comprometer a segurança nacional, especialmente em setores de defesa e infraestrutura crítica (Chapple, 2021).

c. Interrupções Operacionais: Ataques que comprometem a funcionalidade de sistemas de controle e automação podem resultar em falhas catastróficas em processos industriais. Por exemplo, a desativação de sistemas de controle em uma planta de energia pode causar acidentes e riscos à segurança pública (NIST, 2020). Além das perdas imediatas, essas interrupções podem exigir investigações prolongadas e a implementação de novas medidas de segurança, elevando os custos para as organizações.

É justamente neste cenário de crescentes ameaças cibernéticas que a adoção de redes segregadas de TI se mostra uma estratégia fundamental para mitigar os riscos enfrentados em projetos de engenharia. Ao implementar essa abordagem, as organizações podem fortalecer sua postura de segurança cibernética, protegendo sua infraestrutura de automação operacional, seus dados sensíveis e sigilosos.

Considerando as vulnerabilidades discutidas anteriormente, é possível identificar os seguintes efeitos positivos resultantes da adoção de redes segregadas de TI em projetos de engenharia:

a. Proteção Contra *Ransomware*: a segregação de redes permite que dados críticos sejam isolados de outras partes da infraestrutura de TI, dificultando o acesso para atacantes. Ao segmentar a rede, uma organização pode limitar o impacto de um ataque, assegurando que sistemas críticos permaneçam operacionais, mesmo que outras partes da rede sejam comprometidas. Essa abordagem não apenas protege os dados sensíveis, mas também minimiza o tempo de inatividade, preservando a continuidade dos negócios (Davis; Reiter, 2020).
b. Mitigação de Riscos de Espionagem: redes segregadas podem ser utilizadas para isolar informações críticas e tecnologias sensíveis, limitando o acesso apenas a usuários autorizados, pois, ao se criar zonas de acesso distintas, as organizações podem proteger suas inovações e processos de desenvolvimento contra tentativas de roubo de dados. Essa segregação não só preserva a competitividade institucional, como também garante que informações sigilosas permaneçam seguras (Chapple, 2021).
c. Garantia da Funcionalidade Operacional: a adoção de redes segregadas permite que sistemas de controle essenciais operem de forma independente de outras partes da rede. Isso significa que, mesmo que um setor da rede seja

atacado, os sistemas críticos podem continuar a funcionar, evitando falhas catastróficas. Essa abordagem não apenas protege a integridade operacional, mas também reduz a necessidade de investigações prolongadas e a implementação de medidas corretivas dispendiosas (NIST, 2020).

Tomando como base os projetos estratégicos do SNCA e da PNE, que fazem parte do PROSUB e do PNM, a segregação das redes de computador para desenvolvimento desses projetos é essencial, dada a sensibilidade das informações envolvidas. A adoção de uma arquitetura de rede segregada proporciona o isolamento de dados relacionados à tecnologia nuclear, projetos de engenharia naval e informações operacionais, reduzindo significativamente o risco de espionagem e ataques cibernéticos. Além disso, essa abordagem permite um gerenciamento mais eficaz dos acessos, garantindo que apenas indivíduos autorizados possam acessar informações e sistemas críticos. Essa segurança adicional é particularmente importante em projetos que lidam com tecnologia de ponta e informações estratégicas, minimizando a probabilidade de erros humanos e ações mal-intencionadas.

2.5 Desafios para Atualização e Evolução dos Ativos das Redes Segregadas de TI

A atualização e evolução dos ativos em um ambiente cibernético são fundamentais para garantir a proteção cibernética, haja vista que à medida que novas ameaças surgem, as vulnerabilidades em sistemas, software e hardware também se ampliam, podendo-se citar os principais pontos que ressaltam essa importância:

a. Redução de Vulnerabilidades: a atualização regular de software e sistemas operacionais ajuda a corrigir falhas de segurança que poderiam ser exploradas por atacantes, sendo que, manter os sistemas atualizados é uma das práticas mais eficazes para proteger informações sensíveis (NIST, 2022).
b. Adoção de Novas Tecnologias: a evolução dos ativos cibernéticos permite a implementação de novas tecnologias de segurança que podem melhorar a defesa contra os ataques cibernéticos, sendo que as tecnologias emergentes, como inteligência artificial e aprendizado de máquina, podem oferecer detecções mais rápidas e precisas de ameaças (Gartner, 2020).

c. *Compliance* e Regulamentações: muitas organizações estão sujeitas a regulamentações que exigem atualizações regulares de sistemas para manter a conformidade, protegendo a organização não apenas contra multas, mas também fortalecendo sua postura de segurança (Brasil, 2018b; União Europeia, 2016).
d. Capacitação da Equipe de TI: A atualização de ativos também implica na capacitação contínua da equipe de tecnologia da informação, em que treinamentos regulares garantem que os profissionais estejam cientes das últimas ameaças e das melhores práticas de segurança (NIST, 2024a).
e. Resiliência Organizacional: a capacidade de se adaptar rapidamente a novas ameaças e vulnerabilidades contribui para a resiliência organizacional. Um ambiente cibernético em constante evolução é menos suscetível a ataques bem-sucedidos (CISA, 2024).

Conforme já amplamente demonstrado neste trabalho, a adoção de redes segregadas de TI é uma forma bastante eficaz para proteger informações sensíveis em projetos estratégicos de engenharia. No entanto, a adoção desta arquitetura pode trazer diversas dificuldades que podem impactar sua eficácia, citando-se:

a. Complexidade na Implementação: a criação de uma arquitetura de rede segregada envolve um planejamento meticuloso e um entendimento profundo da infraestrutura existente, haja vista que a implementação pode ser complexa, exigindo a reestruturação da rede atual para acomodar as novas exigências de segurança, onde a complexidade técnica e a necessidade de integração de novos sistemas podem resultar em atrasos e custos elevados durante a implementação (Mason *et al.*, 2018).
b. Integração com Sistemas Legados: a integração de redes segregadas com sistemas legados é um desafio significativo, sendo que muitas vezes, as organizações têm sistemas antigos que não são compatíveis com as novas arquiteturas de segurança, onde a coexistência de tecnologias novas e legadas pode criar vulnerabilidades e complicações operacionais, tornando a segurança da informação mais complexa de se gerenciar (Vallabh *et al*., 2020).
c. Resistência Cultural e Organizacional: a resistência à mudança é uma barreira comum na adoção de novas tecnologias, haja vista que as equipes podem

estar habituadas a um ambiente de rede integrado e podem relutar em adotar uma abordagem segregada, onde a mudança organizacional frequentemente enfrenta resistência, especialmente quando a nova abordagem é vista como complexa ou desnecessária (Kotter, 1996).

d. Gerenciamento de Acesso e Autenticação: a implementação de controles de acesso eficazes é fundamental em uma rede segregada sendo que, porém, o gerenciamento de múltiplos níveis de acesso e autenticação pode ser um processo complexo, aumentando o risco de configurações incorretas que podem comprometer a segurança da rede (Murray *et al*., 2019).

e. Monitoramento e Manutenção: as redes segregadas exigem monitoramento contínuo para detectar e responder a possíveis ameaças, sendo que essa demanda adicional pode sobrecarregar as equipes de TI, que precisam de recursos adequados para garantir a segurança, onde a manutenção de redes segregadas requer uma abordagem proativa, o que pode não ser viável em ambientes com recursos, humanos e tecnológicos, limitados (Kumar *et al.*, 2021).

f. Custos Associados: os custos associados à implementação e manutenção de redes segregadas podem ser significativos, pois, além do investimento inicial em infraestrutura, há custos recorrentes relacionados à manutenção e atualização dos sistemas, sendo que, em contextos onde os recursos são escassos, esses custos podem ser um impedimento para a adoção de práticas de segurança robustas (Almgren *et al*., 2017).

g. Inovação Contida: estudos indicam que a inovação é frequentemente impulsionada pela troca de ideias e pela colaboração interdisciplinar (Chesbrough, 2003), sendo que inovação contida se refere à limitação da criatividade e do intercâmbio de ideias em ambientes altamente segregados. Embora a segregação de redes aumente a segurança contra ameaças cibernéticas (NIST, 2020), ela pode criar barreiras à colaboração, dificultando o compartilhamento de informações e a adoção de novas tecnologias, onde a falta de interação entre diferentes setores leva a uma resistência à inovação, o que pode comprometer a atualização de sistemas e a integração de novos ativos.

h. Comprometimento da Tomada de Decisão: informações isoladas em redes distintas afetam a capacidade de obter uma visão holística do ambiente de TI,

o que pode impactar tanto a velocidade quanto a qualidade das decisões tomadas, resultando em processos decisórios mais lentos e menos informados (Kumar; Singh; Sharma, 2018). A necessidade de múltiplas aprovações e a dificuldade em compartilhar dados críticos podem atrasar a implementação de atualizações e melhorias nos ativos.

Projetos estratégicos de engenharia no setor de defesa, como o Projeto do SNCA, dependem amplamente de recursos financeiros governamentais, que estão frequentemente sujeitos a restrições e inconsistências. Essas limitações impactam negativamente o desenvolvimento e a evolução dos ativos de redes segregadas de TI em órgãos públicos, especialmente devido às instabilidades orçamentárias (Maia, 2014). A falta de um planejamento financeiro adequado pode levar à priorização de gastos imediatos em detrimento de investimentos em segurança cibernética (Cameron *et al*., 2016), e a desconexão entre necessidades técnicas e recursos disponíveis dificulta a implementação de tecnologias essenciais (Bryson; Crosby, 2006).

Além disso, mudanças na legislação podem pressionar orçamentos já limitados (NASCIO, 2019). A implantação e sustentação de redes segregadas de TI exigem considerável esforço da equipe de TI, afetando a qualidade dos serviços prestados. A falta de capacitação contínua e a competição interna por recursos podem agravar ainda mais a situação, tornando essencial que os órgãos públicos abordem essas questões para garantir a segurança e a eficácia das operações (Gonzalez *et al.,* 2018; Peters; Pierre, 2004).

2.6 A Manutenção da Proteção Cibernética das Redes Segregadas de TI

Depreende-se no desenvolvimento deste trabalho que a proteção cibernética em projetos estratégicos de engenharia não é apenas uma necessidade técnica, mas uma questão de sobrevivência organizacional. Com os riscos crescentes e as consequências potenciais de falhas de segurança, investir em cibersegurança é essencial para a integridade e o sucesso dos projetos.

Para assegurar a proteção cibernética em redes de TI segregadas, é essencial implementar uma série de práticas que englobem tanto a segurança técnica quanto o treinamento da equipe e a gestão organizacional, sendo que essas práticas devem considerar as especificidades e complexidades inerentes a esse tipo de

arquitetura já abordadas neste trabalho. Dentre as recomendações específicas, destaca-se:

a. Implementação de um cronograma de atualizações regulares de sistemas e *software*: estabelecer um calendário para garantir que todos os sistemas e *softwares* sejam atualizados regularmente, ajudando a reduzir vulnerabilidades conhecidas (NIST, 2022), sendo que esse cronograma deve incluir a análise dos sistemas e softwares utilizados, a integração com o plano de gestão de mudanças (ISO, 2022), a automação do processo de atualização e a comunicação eficaz entre as equipes de TI e os usuários finais. Além disso, é essencial monitorar e ajustar continuamente o cronograma para responder a novas vulnerabilidades e requisitos de segurança (SANS, 2021), garantindo assim a proteção contínua dos dados e sistemas críticos (Verizon, 2023).
b. Avaliação e integração de novas tecnologias de segurança: investir em soluções de segurança baseadas em inteligência artificial e aprendizado de máquina, que podem oferecer detecções e respostas mais rápidas a ameaças (Gartner, 2020), assim como garantir que novas tecnologias sejam compatíveis com sistemas legados para evitar lacunas de segurança (Vallabh *et al*., 2020).
c. Estabelecer um orçamento dedicado e priorizar investimentos em segurança cibernética: garantir que uma parte do orçamento seja reservada especificamente para atualizações de segurança e tecnologia, além de desenvolver uma estratégia de priorização que considere os riscos e a criticidade das informações a serem protegidas (Cameron *et al.,* 2016).
d. Capacitar continuamente a equipe de TI e simular incidentes cibernéticos: realizar treinamentos regulares para a equipe de TI, focando em novas ameaças e melhores práticas de segurança (NIST, 2024a), assim como conduzir exercícios práticos que simulem ataques cibernéticos para preparar a equipe a responder adequadamente (SANS, 2018a).
e. Implementar Controle de Acesso Baseado em Funções (RBAC) e Autenticação Multifatorial (MFA): Definir permissões de acesso de acordo com as funções dos usuários, minimizando a exposição a dados sensíveis e implementação de múltiplas formas de autenticação para acesso a sistemas críticos, aumentando a segurança (NIST, 2014; NIST, 2017a; ISO, 2022).

f. Monitorar continuamente e em tempo real da rede: adotar ferramentas que ofereçam monitoramento contínuo para detectar e responder a ameaças em tempo real através de, por exemplo, a implementação de uma prática rigorosa de análise de logs para identificar comportamentos suspeitos ou anômalos (CISA, 2024).

g. Desenvolver um plano de resposta a incidentes e avaliação regulares de risco: criar e manter um plano que detalhe os protocolos a serem seguidas em caso de um ataque cibernético (NIST, 2012b), assim como realizar avaliações regulares de risco através da análise periódica de risco para se adaptar as novas ameaças e vulnerabilidades (NIST, 2012a).

h. Fomentar a colaboração entre equipes e estabelecer canais de comunicação bem definidos: criar um ambiente onde equipes de TI que atuam na sustentação de diferentes ambientes computacionais possam compartilhar informações sobre vulnerabilidades e ameaças (NIST, 2013), assim como estabelecer protocolos de comunicação claros para reportar incidentes e questões de segurança (SANS, 2018b).

i. Gerenciar a complexidade dos ativos cibernéticos: manter documentação detalhada sobre a arquitetura da rede e as políticas de segurança (NIST, 2011), facilitando a compreensão e a gestão, assim como utilizar ferramentas que ajudem a gerenciar e monitorar a configuração dos sistemas, garantindo que as alterações sejam registradas e revisadas (ISO, 2022).

j. Conscientizar continuamente os usuários sobre a segurança cibernética: apesar das robustas medidas tecnológicas implementadas, o comportamento dos usuários continua a ser um fator crítico para a segurança cibernética, sendo essencial fortalecer a mentalidade de segurança cibernética a fim de mitigar vulnerabilidades internas, como erros humanos e ameaças maliciosas. Neste cenário, programas de treinamento contínuos, simulações de incidentes e implantação de políticas de segurança da informação são fundamentais para garantir que os usuários compreendam a importância da proteção das informações sensíveis (Bada; Sasse; Nurse, 2019; NIST, 2017a). A cultura organizacional também desempenha um papel vital nesta tarefa, com a liderança promovendo uma postura de segurança que se alinha às metas estratégicas da organização, assegurando a integridade dos ativos críticos e a continuidade dos projetos (Kotter, 1996; Chapple, 2021; NIST, 2024a).

Considerando as características dos projetos estratégicos em engenharia, a sensibilidade das informações e os riscos relacionados a falhas de segurança podem acarretar consequências comprometedoras para a execução do projeto, como exemplificado no caso do Projeto do SNCA. As práticas apresentadas não devem ser vistas apenas como recomendações convencionais, mas como uma necessidade estratégica essencial para assegurar a integridade e a segurança de um empreendimento tão complexo e crítico. Essa abordagem integrada demonstra ser promissora na proteção contra ameaças cibernéticas, visando garantir o sucesso do projeto a longo prazo.

3 CONSIDERAÇÕES FINAIS

Este estudo demonstrou que a implementação de redes segregadas de TI em projetos estratégicos de engenharia, especialmente na defesa nacional, é crucial para garantir a segurança cibernética em ambientes sensíveis. O Projeto do SNCA foi utilizado como referência para a importância de proteger informações críticas e isolar ativos digitais para mitigar riscos de espionagem, ataques cibernéticos e comprometimentos operacionais.

A atualização e evolução dos ativos tecnológicos nessas redes representam um desafio constante, exigindo planejamento contínuo, investimentos em infraestrutura e capacitação técnica adequada. A gestão eficaz dessas redes requer soluções tecnológicas robustas e uma abordagem organizacional integrada, que envolva políticas de segurança, treinamento de equipes e monitoramento de ameaças emergentes.

As análises indicam que, apesar das dificuldades, a adoção de redes segregadas oferece vantagens significativas em segurança e controle, especialmente quando acompanhada de práticas de gestão de riscos e planejamento estratégico. É essencial integrar novas tecnologias de segurança, monitorar continuamente as ameaças, priorizar investimentos em proteção cibernética, e capacitar as equipes de TI, promovendo a conscientização sobre segurança cibernética entre os usuários.

Além disso, este estudo se concentrou em propostas técnico-conceituais para mitigar desafios relacionados à adoção de redes segregadas de TI, sem abordar tecnologias ou métodos específicos. Futuros aprofundamentos podem avaliar o

impacto da inteligência artificial (IA) na gestão dessas redes, pois a IA pode aprimorar a segurança e a eficiência ao automatizar a detecção de ameaças e permitir respostas proativas. Assim, com uma abordagem estratégica, a proteção cibernética em redes segregadas não só garante a integridade dos ativos sensíveis, mas também assegura a continuidade e o sucesso de projetos essenciais para a soberania e segurança nacional.

REFERÊNCIAS

ALMGREN, M. *et al*. Cost Analysis of Network Segregation Strategies. **Journal of Network and Computer Applications**, Amsterdam, v. 107, n.2, p. 55-66, Feb. 2017.

BADA, A.; SASSE, A.; NURSE, J. **Cybersecurity Awareness and the Role of Education. Journal of Cybersecurity and Privacy**, Basel, v. 1, n. 1, p. 80-99, Mar. 2019.

BRASIL. Comando da Marinha. Diretoria-Geral do Material da Marinha. **DGMM-0540**: Normas Sobre Tecnologia da Informação da Marinha. Rio de Janeiro: DGMM, 2019.

BRASIL. Comando da Marinha. Estado-Maior da Armada. **Plano Estratégico da Marinha 2040**. Brasília, DF: EMA, 2020a.

BRASIL. Comando da Marinha. Programa de Desenvolvimento de Submarinos. **Marinha avança na construção do Submarino Nuclear Convencionalmente Armado**. Brasília, DF: MB, 2024a. Disponível em: https://www.marinha.mil.br/prosub/node/384. Acesso em: 18 set. 2024.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 18 set. 2024.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2023a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11856.htm. Acesso em: 18 set. 2024.

BRASIL. **Lei nº 13.709, de 14 de dezembro de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF:

Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2024.

BRASIL. Ministério da Defesa**. Estratégia Nacional de Defesa**. Brasília, DF: MD, 2024b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/estrategia-nacional-de-defesa. Acesso em: 16 set. 2024.

BRASIL. Ministério da Defesa**. Política Nacional de Defesa. Estratégia Nacional de Defesa**. Brasília, DF: MD, 2020b.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria Nº 093, de 18 de outubro de 2021. Aprova o glossário de segurança da informação. **Diário Oficial da União**: seção 1, Brasília, DF, p. 36, 19 out. 2021.

BRYSON, J. M.; CROSBY, B. C. Building a Model of the Public Sector: A Study of the Role of Leadership in the Evolving Nature of Public Sector Organizations**. Public Administration Review**, Washington, D.C., v. 66, n. 4, p. 180-195, ago. 2006.

CAMERON, K. S. *et al*. Organizational effectiveness: a comparative analysis of different approaches. **International Journal of Public Administration**, New York, v. 39, n. 9, p. 300-315, Sept. 2016.

CHAPPLE, M. **The Complete guide to cybersecurity for engineering projects**. Amsterdam: Syngress, 2021. 276 p.

CHESBROUGH, H**. Open Innovation**: the new imperative for creating and profiting from technology. Boston: Harvard Business School Press, 2003. 256 p.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Infrastructure Resilience Planning Framework (IRPF)**. Washington, DC: CISA, 2024.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Ransomware Guide**. Washington, DC: CISA, 2020.

DAVIS, J.; REITER, H. **Cybersecurity for engineers**: a guide to protecting your projects. New Jersey: Wiley, 2020. 352 p.

DUNCAN, D.; LEVESON, N.; LOUGH, S. Cybersecurity and systems engineering: a cross-disciplinary approach. **Systems Engineering**, New Jersey, v. 23, n. 2, p. 180-195, Apr. 2020.

FOWLER, M. **Patterns of enterprise application architecture**. Boston: Addison-Wesley Professional, 2002. 560p.

GARTNER. **Market guide for security information and event management**. Stamford: Gartner, 2020.

GONZALEZ, R. *et al.* Cybersecurity Training: A Critical Component of National Security. **Journal of Cyber Policy**, Londres, v. 3, n. 2, p. 80-95, out. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001:2022(E)**: information security, cybersecurity and privacy protection: information security management systems: requirements. Geneve: ISO/IEC, 2022.

GREY, Clifford F.; LARSON Erick W. **Gerenciamento de projetos**: o processo gerencial. Tradução: Théo Amon. 6. ed. Porto Alegre: AMGH, 2016. 608 p.

KOTTER, J. P. **Leading Change**. Boston: Harvard Business Review Press, 1996. 187 p.

KUMAR, A.; SINGH, A.; SHARMA, A. Impact of Organizational Structure on Decision-Making. **International Journal of Management Studies**, Berlin, v. 5, n. 1, p. 45-56, Jan. 2018.

KUMAR, A. *et al.* Proactive Monitoring in Segregated Networks**. International Journal of Information Security**, Berlin, v. 20, n. 2, p.45-60, abr. 2021.

LIU, Y.; CHEN, H. Design and Implementation of a Segregated Network Architecture. **Journal of Network and Computer Applications**, Amsterdam, v. 107, p. 56-66, 2018.

MASON, J. *et al*. Implementing Network Segregation: Challenges and Strategies. **Cybersecurity Review**, London, v. 5, n. 3, p. 101-115, May 2018.

MAIA, Robert Marques. **Virtualização em Redes de Computadores**: estudo de caso de implantação da tecnologia no PRODABEL baseado em um novo paradigma, seus desafios e resultados. 2014. Trabalho de Conclusão de Curso (Pós-Graduação em Redes de Computadores) – Universidade Nove de Júlio, São Paulo, 2014.

MURRAY, P. *et al.* Access Management in Segregated Networks. **Information Systems Journal,** Hoboken, v. 29, n. 4, p. 200-215, June 2019.

NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS. **State IT Budget Trends**: 2018-2019. Washington, DC.: NASCIO, 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **Federal Information Processing Standards Publication 197**: Advanced Encryption Standard (AES). Gaithersburg: NIST, 2001.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-30 Revision 1**: Guide for Conducting Risk Assessments. Gaithersburg: NIST, 2012a.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-34 Revision 1**: Contingency Planning Guide for Federal Information Systems. Gaithersburg: NIST, 2010.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-40 Revision 4**: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. Gaithersburg: NIST, 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-41 Revision 1**: Guidelines on Firewalls and Firewall Policy. Gaithersburg: NIST, 2009.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-50 Revision 1**: Building a Cybersecurity and Privacy Learning Program. Gaithersburg: NIST, 2024a.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-53 Revision 5**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES**. NIST Special Publication 800-61 Revision 2**: Computer Security Incident Handling Guide. Gaithersburg: NIST, 2012b.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES**. NIST Special Publication 800-63-3**: Digital Identity Guidelines. Gaithersburg: NIST, 2017a.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES**. NIST Special Publication 800-63B**: Digital Identity Guidelines: Authentication and Lifecycle Management. Gaithersburg: NIST, 2017b.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES**. NIST Special Publication 800-83 Revision 1**: Guide to Malware Incident Prevention and Handling for Desktops and Laptops. Gaithersburg: NIST, 2013.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-94 Revision 1**: Guide to Intrusion Detection and Prevention Systems (IDPS). Gaithersburg: NIST, 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-128**: Guide for Security-Focused Configuration Management of Information Systems. Gaithersburg: NIST, 2011.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **NIST Special Publication 800-162**: Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Gaithersburg: NIST, 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES. **The NIST Cybersecurity Framework (CSF) 2.0**. Gaithersburg: NIST, 2024b.

PETERS, B. G.; PIERRE, J. The Role of Public Administration in Democratic Governance. **Governance**, [S./.], v. 17, n. 3, p. 335-354, July 2004.

SANS INSTITUTE. **Segregation of Duties in IT Security**. Bethesda: Sans Institute, 2019.

SANS INSTITUTE. **The Importance of Cybersecurity Exercises**. Bethesda: Sans Institute, 2018a.

SANS INSTITUTE. **The Importance of Collaboration in Cybersecurity.** Bethesda: Sans Institute, 2018b.

SANS INSTITUTE. **Top 20 Critical Security Controls for Effective Cyber Defense.** Bethesda: Sans Institute, 2021.

STALLINGS, W. **Network Security Essentials**: Applications and Standards. 6. ed. Essex: Pearson, 2020. 464 p.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores**. Tradução: Daniel Vieira. 5. ed. Porto Alegre: Pearson, 2021. 568 p.

TANENBAUM, Andrew S.; AUSTIN, Todd. **Structured Computer Organization**. 6. ed. Essex: Pearson, 2013. 808 p.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abr. de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Diário Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 25 set. 2024.

VALLABH, S. *et al*. Legacy Systems and Security Challenges. **Computer Security**, Amsterdam, v. 39, n. 7, p. 150-165, July 2020.

VERIZON. **2023 Data Breach Investigations Report**. New York: Verizon, 2023.

WIENER, Norbert. **Cibernética e Sociedade**: o uso humano de seres humanos. Tradução: José Paulo Paes. 2. ed. São Paulo: Cultrix, 1968. 190 p.

ZWICKY, E. D.; COOPER, S.; CHAPMAN, D. **Building Internet Firewalls**. Sebastopol: O'Reilly Media, 2000. 894 p.