Arquitetura de segurança para sistemas críticos digitais do governo brasileiro: uma análise baseada no modelo nuclear

Aléxis dos Santos França, Éder Souza Gualberto

Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - CEP 70910-900

alexis.franca@aluno.unb.br, edermiguel@unb.br

Abstract*: This article examines the application of computer security concepts from the nuclear sector as a reference for critical digital systems in the Brazilian government. The objective is to assess how principles such as defense in depth and the graded approach can strengthen the Privacy and Information Security Program (PPSI). The research, applied in nature and comparative in scope, was based on a bibliographic and documentary review of international standards and guidelines, as well as national regulations. Convergences, gaps, and opportunities between PPSI controls and nuclear concepts were analyzed. The results indicate strong alignment, enabling the proposal of preliminary security architecture guidelines adaptable to the Brazilian governmental context.*

Resumo: *Este artigo examina a aplicação de conceitos de segurança computacional do setor nuclear, como referência para sistemas críticos digitais do governo brasileiro. O objetivo é avaliar como princípios como defesa em profundidade e abordagem graduada podem fortalecer o Programa de Privacidade e Segurança da Informação (PPSI). A pesquisa, de natureza aplicada e caráter comparativo, baseou-se em revisão bibliográfica e documental de normas e padrões internacionais, bem como normativos nacionais. Foram analisadas convergências, lacunas e oportunidades entre os controles do PPSI e os conceitos nucleares. Os resultados indicam boa aderência, permitindo propor diretrizes preliminares de arquitetura de segurança adaptáveis ao contexto governamental brasileiro.*

1. Introdução

Nas últimas décadas, a administração pública brasileira tem experimentado um processo acelerado de transformação digital, impulsionado tanto por demandas sociais por serviços mais ágeis e acessíveis quanto por iniciativas governamentais de modernização do Estado. O Brasil se tornou um dos líderes mundiais em governo eletrônico, com destaque na oferta de serviços públicos digitais diversos através da plataforma GOV.BR. (BRASIL, 2019).

Essa incorporação crescente de Tecnologia da Informação (TI) nos processos administrativos e operacionais de órgãos públicos, tornou esses sistemas elementos centrais na prestação de serviços essenciais à população. Sistemas de saúde, segurança, justiça, previdência social, arrecadação e controle de recursos públicos operam hoje com

forte dependência de tecnologias digitais interconectadas. Qualquer falha ou comprometimento nesses sistemas podem afetar a capacidade do Estado de cumprir com suas funções, resultando em graves consequências ao país.

Essa elevada importância permite considerá-los como infraestruturas críticas, baseado na definição da Política Nacional de Segurança de Infraestruturas Críticas – PNSIC (Decreto nº 9.573, 2018). A PNSIC também define a segurança de infraestruturas críticas como um conjunto de medidas com o objetivo de preservar ou reestabelecer os serviços relacionados à essas infraestruturas.

No contexto do governo digital brasileiro, as ameaças cibernéticas representam hoje um dos principais vetores de risco para a continuidade, integridade e confiabilidade dos serviços públicos digitais. Com o aumento da superfície de ataque digital e o crescente número de vulnerabilidades identificadas, riscos de interrupções, exposição de dados sensíveis além perdas operacionais e financeiras de grande escala podem causar impactos reais sobre a vida do cidadão, a eficiência da máquina pública e a credibilidade das instituições.

A proteção desses serviços públicos digitais, especialmente os classificados como críticos, exige uma abordagem de segurança estruturada, que vá além da proteção tradicional e incorpore princípios de resiliência, segmentação, gestão de riscos e governança estratégica.

Nesse sentido, por sua natureza de alto risco, o setor nuclear consolidou metodologias de segurança rigorosas e eficazes, refletidas nas publicações da Agência Internacional de Energia Atômica (AIEA). Na área de segurança computacional, é amplamente utilizado o modelo conceitual denominado *Defensive Computer Security Architecture* (DCSA), onde são aplicados controles proporcionais em diferentes níveis de segurança no ambiente baseados nos riscos envolvidos.

Este trabalho, assim, pretende realizar uma análise dos principais conceitos de segurança cibernética aplicados às instalações nucleares internacionalmente, avaliando sua aderência na construção de uma arquitetura de segurança aplicável aos sistemas críticos de TI da administração pública federal, em conformidade com os objetivos do Programa de Privacidade e Segurança da Informação (PPSI).

2. Referencial Teórico

2.1. Governo digital

Um governo digital pode ser definido pelo emprego de tecnologias de informação e comunicação (TICs) na prestação direta de serviços públicos, com foco na promoção de direitos sociais (CRISTÓVAM, 2020).

No caso do governo brasileiro, ele é acessado através da plataforma GOV.BR, instituída a partir do Decreto nº 9.756, de 11 de abril de 2019 e que inclui diversos serviços e informações em um único portal. Essa oferta centralizada de serviços públicos digitais permite que os cidadãos interajam com o Estado de forma direta, ágil e acessível à

população, sem a necessidade de deslocamento físico, contribuindo para a democratização do acesso e para a eficiência da gestão pública.

Esses serviços são entregues através do emprego de diferentes TICs, incluindo robustos sistemas de informação (SI). Um sistema de informação é um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem informações para apoiar a tomada de decisões e o controle em uma organização. (O'BRIEN; MARAKAS, 2021).

Com o aumento no uso de serviços públicos digitais, os sistemas de computação que o suportam passam a processar grandes volumes de dados pessoais e sensíveis, como informações de saúde, dados previdenciários, registros fiscais, entre outros.

Nesse cenário, a segurança da informação (SegInfo) se torna um pilar fundamental. De acordo com o NIST (2020), segurança da informação é a proteção de informações e sistemas de informação contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de fornecer confidencialidade, integridade e disponibilidade.

Além disso, a segurança da informação visa proteger a informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar riscos e maximizar o retorno sobre os investimentos (ABNT, 2022).

No contexto dos serviços públicos digitais, a Secretaria de Governo Digital (SGD) do governo do Brasil estabeleceu um Programa de Privacidade e Segurança da Informação – PPSI através da Portaria SGD/MGI n. 852 (BRASIL, 2023), com objetivo elevar a maturidade e a resiliência cibernética dos órgãos governamentais federais. O PPSI possui um *framework* de privacidade e segurança da informação, inspirado no *CIS Critical Security Controls Version 8* (CIS v8) e que possui um conjunto de controles e salvaguardas para proteção dos serviços digitais contra ataques cibernéticos.

2.2. A segurança computacional no mundo nuclear

A segurança computacional (*computer security*), também comumente denominada segurança cibernética (SegCiber) ou cibersegurança (*Cybersecurity*), é o subconjunto de Segurança da Informação que se preocupa com a proteção de sistemas de computação (*computer based systems*) contra seu comprometimento (IAEA, 2021), conforme ilustrado na Figura 1.

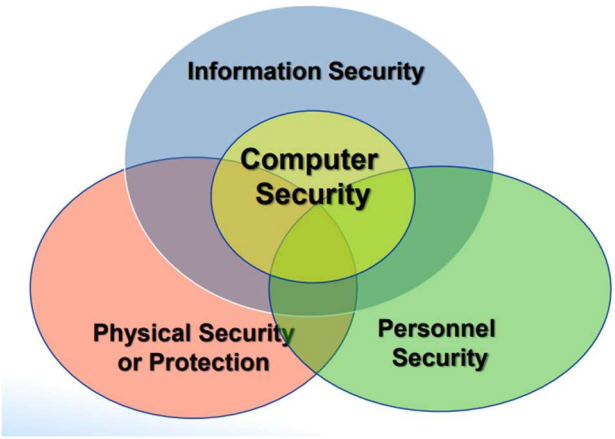

Figura 1. domínios de segurança nuclear. Fonte: IAEA

No setor nuclear, sistemas de computação utilizados para proteção física, segurança nuclear e contabilidade de material nuclear devem ser protegidos com base em uma avaliação de ameaças (IAEA, 2011). Esses sistemas são compostos por ativos digitais que armazenam e processam informações com diferentes níveis de criticidade.

A criticidade dos ativos está diretamente relacionada com a sensibilidade da informação que ele processa, a função desempenhada pelo sistema que ele pertence e o potencial efeito na segurança e proteção nuclear, em caso de comprometimento. Esse processo de identificação e classificação de criticidade de sistemas e ativos ocorre de forma sistemática. Os ativos digitais considerados críticos são denominados Ativos Digitais Sensíveis (*Sensitive Digital Assets)*.

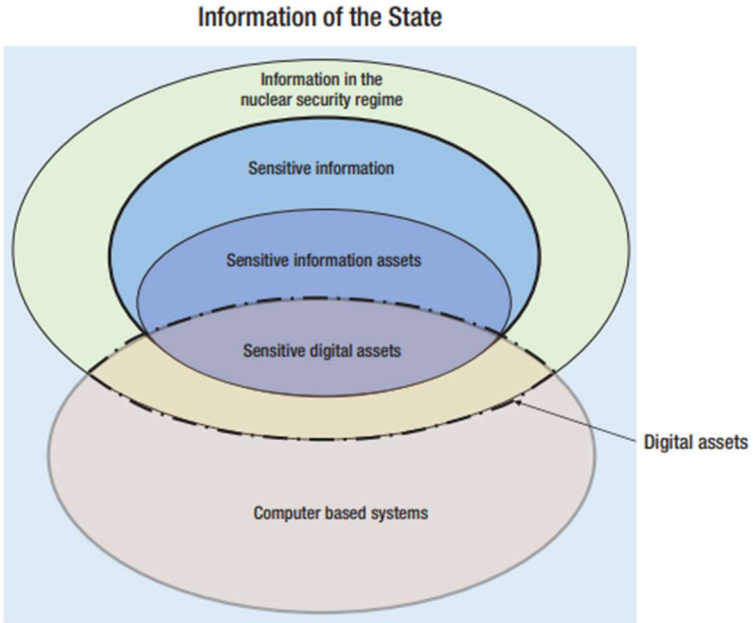

Figura 2. Relação entre sistemas de computação, informações sensíveis e ativos digitais sensíveis. Fonte: IAEA NSS 17-T

2.3. A relação entre o PPSI e a segurança computacional nuclear

Para o aumento da segurança e resiliência dos sistemas digitais federais, o *framework* do PPSI estabeleceu dentre os seus 31 controles de cibersegurança e privacidade, medidas relacionadas à proteção da arquitetura e infraestrutura de rede. Os controles 12 – Gestão da infraestrutura de rede e 13 – Monitoramento e defesa da rede estabelecem premissas a serem cumpridas com objetivo de proteger as redes contra ataques cibernéticos. A tabela 1 a seguir apresenta algumas dessas medidas relacionadas.

Tabela 1. Medidas de gestão da infraestrutura, monitoramento e defesa de Rede. Fonte: PPSI

ID	MEDIDA	DESCRIÇÃO DA MEDIDA
12.1	O órgão elabora e mantém diagramas de arquitetura?	Elaborar e manter diagramas e demais documentações da arquitetura de rede da organização. A revisão destas documentações deve ser realizada de forma periódica ou quando ocorrerem mudanças que possam impactar tais artefatos.
12.3	O órgão garante níveis de segurança para a arquitetura de rede?	Garantir que a arquitetura de rede se mantenha segura. É interessante buscar implementar políticas de segurança como segmentação de rede, privilégio mínimo e níveis básicos de disponibilidade.
13.1	O órgão realiza filtragem de tráfego entre os segmentos de rede?	Realize a filtragem de tráfego entre os segmentos de rede.

A preocupação em estruturar arquiteturas digitais seguras não é exclusiva do contexto governamental brasileiro. Em setores altamente sensíveis, como o nuclear, essa abordagem é igualmente essencial e ganha ainda maior rigor em razão do impacto potencial de falhas de segurança. Nesse sentido, observa-se uma convergência entre os princípios do PPSI e as recomendações internacionais: ambos buscam assegurar que a arquitetura de rede seja planejada, monitorada e defendida de forma sistemática contra ameaças.

De forma semelhante ao que ocorre no âmbito federal, o setor nuclear também consolidou diretrizes específicas para a proteção de ativos digitais críticos. Agência Internacional de Energia Atômica publicou o documento NSS No. 42-G *Computer Security - Implementing Guide*, com objetivo de estabelecer e aprimorar medidas de segurança para a proteção de ativos digitais com foco em instalações nucleares. O documento apresenta o modelo conceitual *Defensive Computer Security Architecture* (DCSA) para aplicação de princípios de segurança, incluindo os conceitos de abordagem graduada (*graded approach*) e defesa em profundidade (*defence in depth*).

2.4. Conceitos fundamentais

O conceito de abordagem graduada é uma estratégia que ajusta o rigor e a complexidade das medidas de segurança de acordo com:

- A importância da função associada aos ativos digitais sensíveis (*SDA*'s);
- O potencial impacto de um comprometimento desses ativos;
- A probabilidade de ocorrência de ameaças.

A adoção de *graded approach* exige, portanto, prévia identificação dos ativos e avaliação de riscos associados a cada sistema e função a ser protegida. A ênfase está na proteção da função, não do ativo isoladamente. O conceito de abordagem graduada considera a limitação de recursos (pessoal, financeiros e de tempo) em um cenário real, possibilitando maior eficiência na alocação destes.

A abordagem gradual considera que devem existir diferentes níveis de segurança computacional (*computer security levels*). Cada nível de segurança possui um nível de proteção, alcançado a partir da aplicação progressiva de conjuntos de medidas de segurança. As funções, sistemas e ativos digitais são classificados nos diferentes níveis, conforme ilustra a Figura 3.

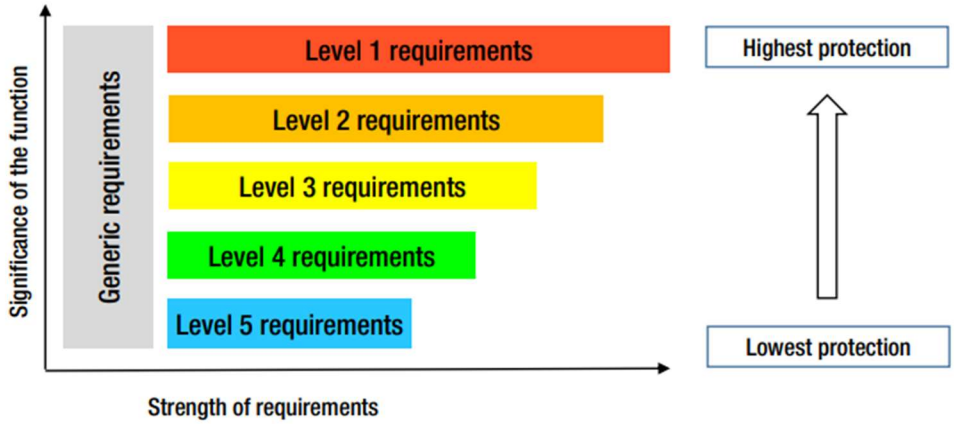

Figura 3. Ilustração da abordagem gradual utilizando níveis de segurança. Fonte: IAEA NSS 42-G

O conceito de defesa em profundidade consiste na adoção de múltiplas camadas e medidas de segurança (técnicas, físicas e administrativas) para a proteção de sistemas digitais. Essas camadas e medidas devem ser combinadas de maneira que caso algum mecanismo de proteção falhe ou seja contornado em uma camada, outros mecanismos sejam capazes de detectar e responder uma violação de segurança (IAEA, 2021). Com *defence in depth*, uma vulnerabilidade de segurança em um computador não deve permitir que um adversário contorne sistematicamente várias camadas de defesa em profundidade.

Muitas arquiteturas de cibersegurança, como a IEC 62443-3-3 - *System Security Requirements and Security Levels* e o NIST SP 800-82r3 - *Guide to Operational Technology* (OT) incorporam os princípios de defesa em profundidade.

A IAEA definiu o modelo *Defensive Computer Security Architecture* (DCSA) como uma forma prática de aplicar os conceitos mencionados de maneira geral, incluindo em

segurança de rede. A Figura 4 apresenta um exemplo com 5 níveis de segurança computacional.

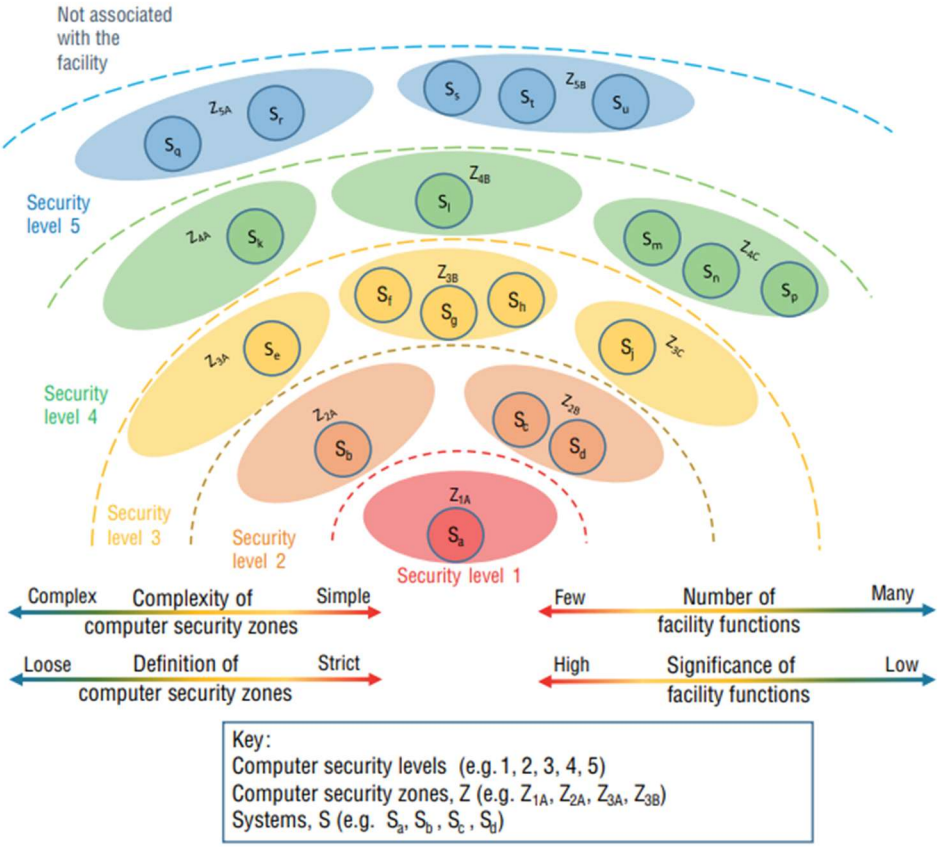

Figura 4. Modelo conceitual de níveis e zonas de segurança computacional. Fonte: IAEA NSS 17-T

Como pode ser observado na Figura 4, as camadas sucessivas de medidas de segurança computacional devem ser superadas ou contornadas por um adversário para comprometer sistemas que realizam funções mais importantes. A especificação da DCSA exige uma mistura planejada de medidas de controle técnicas, físicas e administrativas para proporcionar defesa em profundidade. Cada organização deve estabelecer uma definição do que cada nível representa e como medir o nível de segurança da zona. Essa definição ou caracterização deve ser usada de forma consistente em toda a organização (IAEA, 2021).

Para a correta implementação, o modelo possui algumas premissas. As funções com maior significância devem ser atribuídas ao nível mais rigoroso. Nos níveis mais rigorosos, comunicações entre diferentes níveis são desaconselhadas. Caso seja necessário, convém que elas só possam ser iniciadas pelo menor nível e que possuam medidas de controle, como firewalls ou diodos de dados para restrição de comunicação.

Além disso, é preciso observar as seguintes recomendações:

a) Um nível pode conter uma ou mais funções e zonas;
b) Cada função é atribuída a um único nível;

c) Uma função pode conter uma ou mais zonas;
d) Cada zona é atribuída a um único nível;
e) Uma zona pode conter um ou mais sistemas;
f) Cada sistema pode executar uma ou mais funções (deve ser evitado);
g) Cada sistema é colocado dentro de uma única Zona (sempre que possível).

Uma zona de segurança (*security zone*) consiste no agrupamento de sistemas digitais que possuem afinidade e compartilham requisitos de segurança em comum. Essa abordagem deriva do princípio de *Defence in Depth*, que propõe múltiplas camadas de proteção para dificultar o acesso não autorizado e limitar a propagação de incidentes. De acordo com o NIST (2023), funções críticas em sistemas industriais devem possuir sistemas e componentes em redundância, a fim de evitar ponto único de falha (*single-point-of-failure – SPOF*). Convém, por exemplo, que esses sistemas e componentes redundantes estejam em diferentes zonas de segurança.

3. Metodologia

Este estudo caracterizou-se como uma pesquisa de natureza aplicada, uma vez que tem como objetivo a utilização prática do conhecimento e a resolução de problemas específicos (SILVA; MENEZES,2005).

Dentre os 18 controles de cibersegurança presentes no PPSI, os controles 12 – Gestão da infraestrutura de rede e 13 – Monitoramento e defesa da rede estabelecem uma série de medidas a serem atendidas pelos órgãos federais, com destaque para as medidas relacionadas à elaboração e garantia de níveis adequados de segurança em arquitetura de redes.

Apesar de bem definidos os requisitos, o *Framework* do PPSI não define como implementar as medidas. Essa abordagem não prescritiva permite que cada órgão atinja o cumprimento do requisito considerando as peculiaridades do seu ambiente. Entretanto, a elaboração de diagramas de arquitetura de redes seguras não é uma simples tarefa administrativa. Ela envolve conhecimento especializado para entender os componentes e tecnologias da rede, aplicar princípios de segurança (*Security by design*) e desempenho, além de representar corretamente o ambiente em documentação.

Dessa maneira, o objetivo principal da pesquisa é fornecer diretrizes de arquitetura de segurança aplicáveis aos serviços públicos digitais críticos da administração pública federal, contribuindo dessa maneira com o sucesso do PPSI.

Através de uma revisão bibliográfica e documental utilizando como critério de seleção de fontes as principais publicações relacionadas no tema segurança computacional (*computer security*) por organizações mundialmente reconhecidas no setor nuclear e que fornecem padrões de fato na indústria, tais como IAEA, NIST, ISO e IEC, além de marcos normativos brasileiros sobre o tema, a pesquisa possuiu caráter exploratório e comparativo, buscando identificar oportunidades, lacunas e possíveis adaptações dos conceitos e modelos utilizados para segurança de infraestruturas críticas em relação aos serviços públicos digitais.

Na sequência metodológica, foi feita uma análise comparativa com objetivo de avaliar a aderência das premissas do modelo nuclear DCSA em relação aos requisitos do Programa de Privacidade e Segurança da Informação (PPSI). A partir do resultado dessa análise, onde foram identificadas as convergências e lacunas entre eles, foi proposto um conjunto de diretrizes preliminares de arquitetura de segurança para sistemas críticos governamentais. A figura 5 ilustra as etapas desse processo.

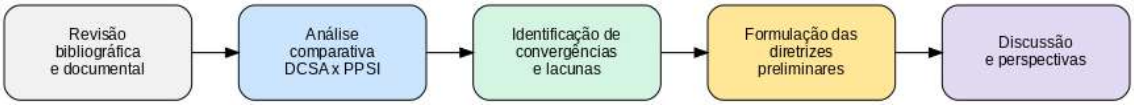

Figura 5. Etapas da metodologia de pesquisa utilizada

4. Resultados e Discussão

Nesta seção, apresentam-se os resultados da análise comparativa entre os conceitos do Defensive Computer Security Architecture (DCSA) da IAEA e os controles do Programa de Privacidade e Segurança da Informação (PPSI), com base na metodologia descrita na Seção 3. A partir dessa análise, avançamos para a formulação de uma proposta preliminar de diretrizes de arquitetura de segurança voltadas a sistemas críticos digitais da administração pública federal. As diretrizes fornecem uma abordagem estruturada que pode contribuir para a elevação da resiliência e maturidade cibernética do Estado brasileiro. Dessa forma, a seção não apenas compara modelos, mas também apresenta recomendações concretas para sua adaptação e aplicação em serviços públicos digitais críticos.

4.1. Análise comparativa

A análise comparativa entre os conceitos de *Defensive Computer Security Architecture* (DCSA) da IAEA e os controles do Programa de Privacidade e Segurança da Informação (PPSI) permite identificar pontos de convergência e lacunas que podem orientar a formulação de diretrizes de arquitetura de segurança aplicáveis a sistemas críticos digitais do governo brasileiro. A Tabela 2 apresenta uma análise de aderência entre os elementos elencados do modelo DCSA e os controles do PPSI de cibersegurança.

Tabela 2. Aderência dos conceitos DCSA x PPSI

Conceito DCSA	Descrição	Controle PPSI	Aderência	Observações
Ativos digitais sensíveis	Identificação e classificação de ativos críticos	Controle 1 - Inventário e Controle de Ativos Institucionais	Alta	Alinhado ao foco em ativos, mas pode ser aprimorado com classificação por impacto no negócio

Abordagem graduada	Ajuste de medidas de segurança baseado na criticidade dos ativos e riscos potenciais	Controle 12 - Gestão da infraestrutura de rede	Média - Alta	O PPSI promove o conceito de segmentação de rede, sem progressividade
Defesa em profundidade	Múltiplas camadas de proteção (técnicas, físicas, administrativas) para mitigar falhas em uma camada	Controle 13 - Monitoramento e defesa da rede	Média	O PPSI aborda de forma simplificada a filtragem entre segmentos como medida
Zonas de segurança computacional	Agrupamento de sistemas com requisitos comuns, com barreiras lógicas/físicas	Controle 12 - Gestão da infraestrutura de rede	Alta	O PPSI promove o conceito de segmentação de rede

De uma forma geral, a análise resultou em uma aderência média-alta, indicando boa compatibilidade entre os conceitos apresentados e os requisitos definidos nos controles do PPSI. Para além da compatibilidade, foram identificados possíveis ganhos potenciais com a integração dos conceitos nucleares.

O controle 1 - inventário e controle de ativos institucionais define a necessidade de estabelecer e manter um inventário de todos os ativos, sem considerar qualquer relação dos ativos mapeados com seus sistemas, funções e riscos associados. Essa limitação pode ser superada pela adaptação do conceito de Ativos Digitais Sensíveis (*Sensitive Digital Assets),* classificando os ativos digitais com base em seu potencial impacto no negócio em caso de violação da cibersegurança.

O controle 12 - gestão da infraestrutura de rede estabelece entre os seus requisitos a necessidade de garantir uma arquitetura de rede segura. Em uma abordagem não prescritiva, o controle sugere a implementação de segmentação de rede, privilégio mínimo e níveis de disponibilidade. Os conceitos de abordagem graduada e defesa em profundidade permitem alcançar esses objetivos de forma progressiva, contribuindo para a conformidade com o programa.

O controle 13 - monitoramento e defesa da rede define, entre outras medidas, a necessidade de filtragem de tráfego entre segmentos de rede. A adoção de zonas de segurança permite agrupar os ativos e filtrar o tráfego entre zonas. Essa implementação também contribui para a abordagem graduada, permitindo aplicar diferentes medidas de segurança de acordo com o nível dos riscos associados às diferentes zonas.

4.2. Uma proposta de diretrizes de arquitetura de segurança

A análise comparativa evidenciou não apenas pontos de convergência entre o modelo nuclear DCSA e os controles do PPSI, mas também revelou oportunidades de aprimoramento que podem fortalecer a segurança de sistemas críticos governamentais. Entre as convergências, destacam-se a ênfase em segmentação de rede e gestão da infraestrutura, presentes no Controle 12 do PPSI e no conceito de zonas de segurança do DCSA. Ambos reconhecem a necessidade de limitar a propagação de incidentes por meio da criação de barreiras lógicas e físicas. Outra aproximação relevante está no princípio da defesa em profundidade, implícito no Controle 13 do PPSI (monitoramento e defesa da rede) e plenamente desenvolvido pela IAEA, com a recomendação de múltiplas camadas de proteção técnica, física e administrativa.

No entanto, algumas lacunas são evidentes. Enquanto a IAEA adota uma abordagem graduada, ajustando o rigor das medidas de segurança conforme a criticidade dos ativos digitais, o PPSI ainda carece de mecanismos claros para classificar ativos com base em impacto e risco. Essa limitação reduz a capacidade de priorização de esforços e investimentos de segurança, sobretudo em um cenário de recursos escassos e crescente demanda por resiliência cibernética na administração pública.

Dessa forma, propõe-se um conjunto de diretrizes preliminares de arquitetura de segurança para sistemas críticos governamentais:

1. Inventário qualitativo de ativos digitais, de formar a permitir que ativos sejam classificados conforme criticidade de funções e impactos potenciais;
2. Segmentação baseada em níveis e zonas de segurança, inspirados nos modelos de segurança em sistemas de controle industriais, de modo a evitar pontos únicos de falha e controlar o tráfego entre os ativos;
3. Aplicação do conceito de abordagem graduada, através da implementação progressiva de controles de segurança, com níveis mais rigorosos destinados a funções críticas;
4. Defesa em profundidade adaptada ao contexto governamental, com a integração de medidas técnicas , administrativas e físicas em múltiplas camadas de proteção;
5. Governança e atualização contínua, com a realização de revisões periódicas da arquitetura em função de novas ameaças.

A implementação dessas diretrizes enfrenta desafios técnicos, culturais e institucionais. Destacam-se a heterogeneidade dos ambientes de TI governamentais, a carência de profissionais especializados em segurança de infraestruturas críticas e a necessidade de alinhar as práticas de cibersegurança com objetivos estratégicos de governo digital. Esses aspectos indicam que as diretrizes propostas devem ser entendidas como um ponto de partida preliminar, passível de ajustes conforme a realidade de cada órgão e a evolução das ameaças, constituindo uma base inicial para discussões futuras sobre a consolidação de arquiteturas de segurança no setor público.

5. Conclusões

A análise realizada evidenciou que os conceitos do *Defensive Computer Security Architecture* (DCSA), amplamente aplicado no setor nuclear, apresentam significativa aderência aos controles de cibersegurança definidos no Programa de Privacidade e Segurança da Informação (PPSI). Entre os principais pontos de convergência, destacam-se a ênfase na segmentação de rede, a adoção de múltiplas camadas de proteção (*defense in depth*) e a necessidade de inventário qualificado de ativos digitais. Esses elementos, quando adaptados ao contexto governamental, podem fortalecer a proteção de serviços digitais críticos e elevar a maturidade cibernética da administração pública.

A adoção de modelos robustos, inspirados em ambientes de alto risco, mostra-se particularmente relevante para o setor público, que enfrenta crescente complexidade de ameaças e dependência de sistemas digitais essenciais. A integração de práticas consolidadas internacionalmente não apenas amplia a resiliência institucional, mas também favorece a priorização de recursos de segurança de acordo com impacto e criticidade.

Por outro lado, este estudo possui limitações inerentes ao seu caráter exploratório. As diretrizes propostas não foram validadas em ambientes reais de implementação, o que evidencia a necessidade de aprofundamentos futuros. Pesquisas posteriores poderão incorporar simulações, estudos de caso ou aplicações-piloto, de modo a avaliar a efetividade, aplicabilidade e custo-benefício das recomendações sugeridas.

As perspectivas de implementação no contexto brasileiro ainda esbarram em desafios técnicos e institucionais, como a heterogeneidade dos ambientes de TI, a escassez de profissionais especializados e a necessidade de alinhar práticas de cibersegurança com objetivos estratégicos de governo digital. Apesar desses obstáculos, a incorporação gradual de modelos inspirados no setor nuclear representa uma oportunidade concreta para consolidar uma cultura de segurança mais madura e resiliente na administração pública.

Este estudo abre caminho para a consolidação de uma arquitetura de segurança referência governamental voltada à proteção de sistemas digitais críticos. Ao adaptar conceitos internacionalmente reconhecidos ao contexto brasileiro, contribui-se para estabelecer uma base conceitual que poderá fortalecer a resiliência cibernética do Estado e servir como ponto de partida para pesquisas acadêmicas mais aprofundadas e validações práticas.

6. Referências Bibliográficas

BRASIL. Decreto nº 9.756, de 11 de abril de 2019. Institui o portal único “gov.br” e dispõe sobre as regras de unificação dos canais digitais do Governo federal. Diário Oficial da União, Brasília, DF, ed. 70, seção 1, p. 5, 12 abr. 2019.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Brasília, DF, n. 226, seção 1, p. 11, 23 nov. 2018.

CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. Governo digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil. Sequência Estudos Jurídicos e Políticos, Florianópolis, v. 41, n. 84, p. 209–242, 2020. Disponível em: https://doi.org/10.5007/2177-7055.2020v43n84p209. Acesso em: 04/08/2025

O'BRIEN, James A.; MARAKAS, George M. Administração de sistemas de informação. 15. ed. Porto Alegre: AMGH, 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. SP 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy. Gaithersburg, MD: U.S. Department of Commerce, 2020. Disponível em: https://doi.org/10.6028/NIST.SP.800-37r2. Acesso em: 04/08/2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022 – Tecnologia da informação – Segurança da informação – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

BRASIL. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI. Diário Oficial da União, Brasília, DF, ed. 62, seção 1, p. 92, 30 mar. 2023.

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls for Effective Cyber Defense. Version 8. East Greenbush, NY: CIS, 2021. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: 06/08/2025

INTERNATIONAL ATOMIC ENERGY AGENCY. Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G.Vienna: IAEA, 2021.

INTERNATIONAL ATOMIC ENERGY AGENCY. Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T (Rev. 1). Vienna: IAEA, 2021.

SILVA, E. L. da; MENEZES, E. M. Metodologia da Pesquisa e Elaboração de Dissertação. 4. ed. Florianópolis, SC: UFSC, 2005.

FOWLER, M. Patterns of Enterprise Application Architecture. Boston: Addison-Wesley, 2002.