FORTALECENDO A SEGURANÇA DA INFORMAÇÃO EM ÓRGÃOS PÚBLICOS: ESTUDO E CONSOLIDAÇÃO DE MODELOS EXISTENTES

Marcos Rodrigues Fernandes*
Erica de Lima Gallindo**
Alexsandro Lima Damasceno**

RESUMO

Este estudo abordou a segurança da informação no contexto dos órgãos públicos federais, com foco na análise e aprimoramento do framework do Programa de Privacidade e Segurança da Informação (PPSI), especialmente nos aspectos de segurança física. Foram analisados diversos modelos de segurança existentes, como NIST, ISO 27001, CIS Controls v8, e comparados com as diretrizes do PPSI. A metodologia consistiu em uma análise documental dos modelos, seguida de uma comparação para identificar medidas ausentes no framework do PPSI, com a finalidade de fortalecer sua abordagem. Os resultados revelaram diversas medidas de segurança física, relacionadas ao controle de acesso, monitoramento, proteção contra ameaças ambientais e segurança de instalações, que poderiam ser incorporadas ao PPSI. A adoção dessas medidas contribuiria para uma proteção mais robusta dos ativos da administração pública. O estudo conclui que o fortalecimento da segurança da informação nos órgãos públicos é essencial para garantir a integridade, confidencialidade e disponibilidade dos dados sensíveis, assegurando a continuidade dos serviços prestados à sociedade.

Palavras-chave: Orgões públicos. Segurança física. Modelos de controle de informaçao.

ABSTRACT

This study focused on information security in the context of federal public institutions, with an emphasis on analyzing and enhancing the Privacy and Information Security Program (PPSI) framework, particularly in terms of physical security. Various existing security models, such as NIST, ISO 27001, and CIS Controls v8, were analyzed and compared with PPSI guidelines. The methodology involved a documentary analysis of these models, followed by a comparison to

* Graduando em Bacharelado em Ciência da Computação, Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE), Aracati, Ceará, Brasil. E-mail: marcos.rodrigues.fernandes06@aluno.ifce.edu.br

** Erica Gallindo é mestre em Ciência da Computação pela Universidade Federal da Paraíba (UFPB), especialista em Formação Pedagógica na Educação Profissional e Tecnológica (IFCE) e graduada em Ciência da Computação pela Universidade Federal da Paraíba (UFPB). Endereço eletrônico:erica.gallindo@ifce.edu.br.

** Alexsandro Lima Damasceno é mestre em Ciência da Computação pela Universidade Federal Rural do Semi-Árido (UFERSA) e graduado em Ciência da Computação pela Universidade Federal Rural do Semi-Árido (UFERSA). Endereço eletrônico:alexandro.lima@ifce.edu.br .

identify missing measures in the PPSI framework in order to strengthen its approach. The results revealed several physical security measures, related to access control, monitoring, protection against environmental threats, and facility security, that could be incorporated into PPSI. Adopting these measures would contribute to a more robust protection of public administration assets. The study concludes that strengthening information security in public agencies is essential to ensure the integrity, confidentiality, and availability of sensitive data, safeguarding the continuity of services provided to society.

1 INTRODUÇÃO

À medida que o crescimento tecnológico se acentua, a digitalização se expande para diversos setores da sociedade contemporânea, exigindo adaptação e normalização dessa nova realidade. Esse processo de transformação, embora gradual, traz inúmeros benefícios, especialmente para os governos, que podem agilizar serviços, reduzir burocracias e mitigar a perda de dados, entre outras vantagens.

No entanto, essa digitalização também apresenta riscos consideráveis. O relatório anual de 2024 do Fundo Monetário Internacional (FMI) revelou que gestoras de ativos, bancos e seguradoras sofreram mais de 20 mil ataques cibernéticos nas últimas décadas, resultando em perdas de aproximadamente U$12 bilhões. Em ambientes governamentais, as falhas de segurança nem sempre geram prejuízos financeiros diretos, mas podem comprometer a imagem institucional e até paralisar serviços essenciais.

No Brasil, um exemplo recente ocorreu em 23 de julho de 2024, quando um grave incidente de segurança cibernética deixou fora do ar o Sistema Eletrônico de Informações (SEI). Segundo a CNN Brasil, o ataque impactou cerca de nove ministérios, impedindo o acesso a dados cruciais. Posteriormente, o grupo hacker FOG reivindicou a autoria do ataque e exigiu U$1,2 milhão para a devolução das informações sequestradas.

Normalmente, há interesses diversos em tais dados, podendo ser ideológico, financeiro ou por simples curiosidade. David (2024) categoriza os invasores em cinco grupos distintos: hacktivistas, movidos por ideologia ou causas sociais, que buscam causar impacto ou chamar a atenção para determinado assunto; script kiddies, que utilizam programas e scripts prontos para perpetuar seus ataques, não necessariamente possuindo conhecimento na área; insiders mal-intencionados, que são indivíduos em posições-chave com acesso privilegiado ao sistema, podendo usá-lo de forma danosa; cibercriminosos profissionais, com foco principal em ativos financeiros, que exploram brechas de segurança, sejam elas digitais ou humanas; e, finalmente, pesquisadores de segurança, que são contratados para encontrar brechas e falhas de segurança a fim de relatá-las e corrigi-las.

Um exemplo de ataque que explora vulnerabilidades é o *phishing*, que utiliza meios falsos, como e-mails, sites e telefonemas, para obter informações da vítima. A engenharia social é um fator que aumenta as chances de sucesso desse golpe, sendo aplicada de diversas formas.

Segundo Fernandes (2023), trata-se de uma técnica que explora a psique humana para obter acesso a informações sensíveis, serviços ou redes.

Esse método se torna atraente para criminosos, pois permite o acesso a informações críticas sem que seja necessário ultrapassar defesas digitais, como quebras de senhas, antivírus ou firewalls. Um relatório publicado pela empresa Kroll, uma multinacional de consultoria de riscos, investigação empresarial e cibersegurança, apontou a engenharia social como um destaque nas questões de ameaças cibernéticas no terceiro trimestre de 2023. Dessa forma, fica claro que o 'hacking humano' representa uma ameaça séria à segurança, e que são necessários métodos para combatê-lo.

Nesse contexto, tornou-se premente a necessidade de se desenvolver meios para proteger os dados da população em geral. Em 2018, foi criada a Lei nº 13.709, de 14 de agosto, conhecida como Lei Geral de Proteção de Dados (LGPD), que define o tratamento adequado para os dados pessoais, sejam eles físicos ou digitais. Isso criou um marco, pois os sistemas de segurança da informação tiveram que se adaptar a essas mudanças. Visando nivelar a segurança no âmbito federal, em 24 de setembro de 2024, foi assinado o Decreto nº 12.198, que visa à implementação de um sistema de segurança digital robusto, criado por meio de metodologias e preceitos já estabelecidos e testados. A implementação desse projeto será gradual, composta por ciclos que serão executados ao longo de três anos (2024 a 2027).

No contexto da Estratégia Federal de Governo Digital, surge o Programa de Privacidade e Segurança da Informação (PPSI) que se apresenta como uma referência específica para a proteção dos órgãos da administração pública federal. O PPSI se fundamentou em diversos modelos internacionais bem conhecidos, tais como o CIS Controls V8 e o NIST Framework.

No entanto, apesar de ser um modelo satisfatório, se constituindo como um referencial robusto de ações relevantes para se tomar no contexto da segurança da informação, existe um ponto em que não há qualquer tipo de cobertura: os aspectos de proteção física. A ausência de controles físicos pode facilitar acessos não autorizados a servidores, roubo de dispositivos e manipulação de infraestruturas críticas, comprometendo a confidencialidade, integridade e disponibilidade das informações.

Diante deste cenário, este estudo teve como objetivo avaliar o PPSI e a viabilidade de integrar modelos e normas complementares ao seu escopo, aprimorando sua abordagem e proporcionando uma solução mais robusta e abrangente. Para isso, foi realizado um levantamento e análise de diversos frameworks de segurança física, culminando na escolha da norma ISO 27002 para ser usada em complemento ao PPSI. Dessa forma, o estudo compara o CIS Controls V8 com a ISO 27002, buscando identificar convergências e complementar o PPSI de maneira eficaz.

Primeiramente, este estudo analisa o framework do PPSI e suas bases conceituais, estabelecendo um entendimento detalhado de sua estrutura e abordagem. Em seguida, são identificadas oportunidades de melhoria no modelo, destacando pontos em que sua aplicação pode ser aprimorada. Com base nessa análise, propõe-se a inclusão de novas medidas ao PPSI, incorporando diretrizes da norma ISO 27002 para fortalecer sua eficácia, principalmente no tocante à segurança

física.

A estrutura deste trabalho está organizada da seguinte forma: a Seção 2 apresenta a fundamentação teórica, enquanto a Seção 3 reúne exemplos de trabalhos relacionados. A metodologia adotada é detalhada na Seção 4. Os resultados e discussões são abordados na Seção 5 e, por fim, as considerações finais são apresentadas na Seção 6.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção, aborda-se os principais conceitos e práticas relacionados à segurança da informação, explorando suas dimensões essenciais, como confidencialidade, integridade e disponibilidade. Serão discutidos os principais modelos e normas que regem a proteção de dados e sistemas, como O *Cis Controls* e a ISO/IEC 27001, e as ameaças e vulnerabilidades mais comuns enfrentadas pelas organizações no ambiente digital. Além disso, são apresentados os mecanismos e técnicas utilizados para mitigar riscos, como criptografia, controle de acesso e autenticação, proporcionando uma base sólida para compreender os desafios e soluções em segurança da informação.

2.1 Segurança da informação

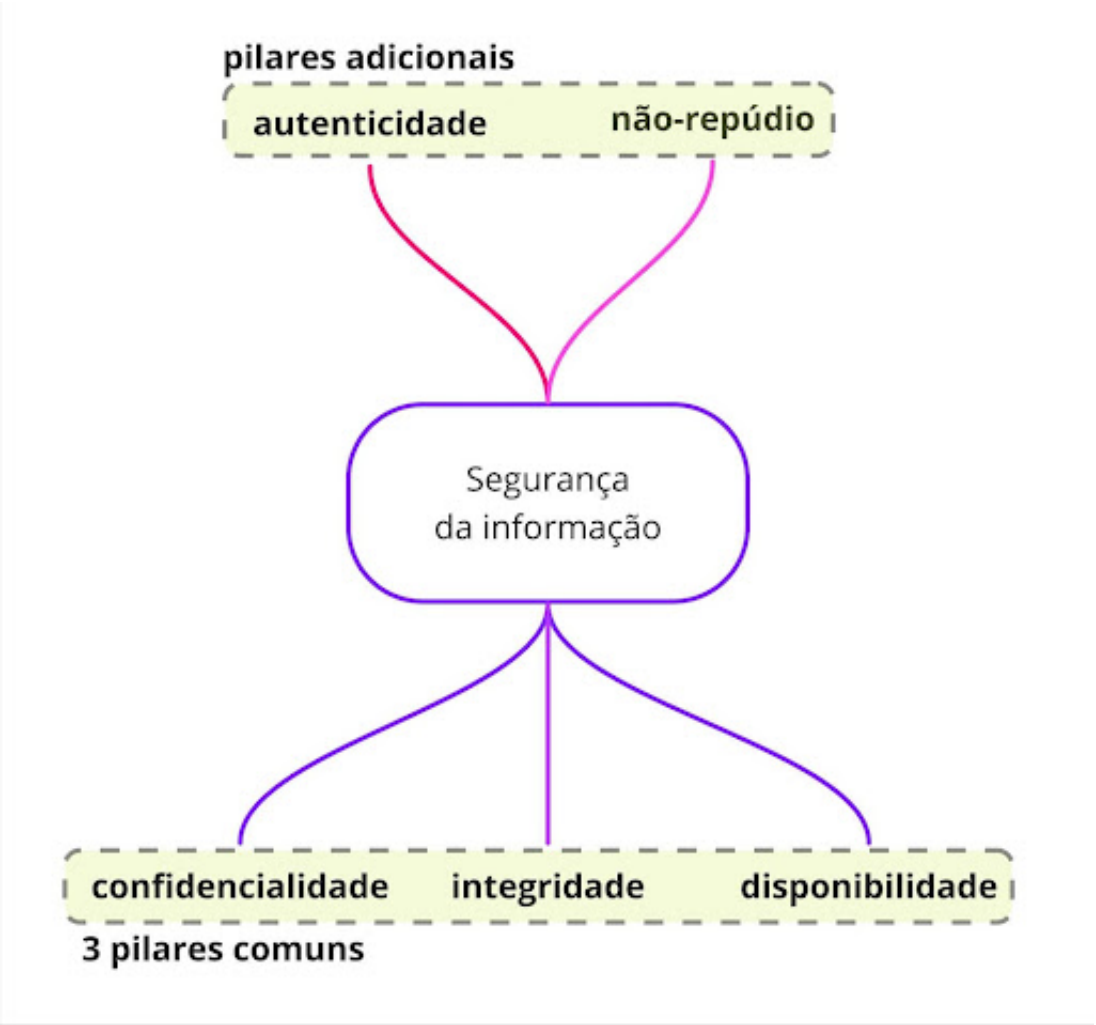
Para falar sobre segurança da informação, é fundamental, primeiramente, contextualizar o que se entende por informação. Segundo Pereira (1996), a informação possui duas dimensões: a pessoal e a coletiva. A dimensão pessoal é afetada pelas experiências individuais, enquanto a coletiva é ajustada pelas percepções do conhecimento coletivo. Para Pinheiros (2004), a informação movimenta-se em um território multifacetado, podendo mudar de significado dependendo da área ou abordagem adotada.

Diante desses conceitos, podemos definir a informação como toda e qualquer forma de dados e conhecimentos reunidos, que pode ser de caráter crítico ou pessoal e apresentar-se de diferentes formas, como digital, física ou pela própria fala humana. Nesse contexto, pode-se inferir que o termo "segurança da informação"refere-se à proteção das informações contra acessos não autorizados, modificações, uso indevido ou interrupções. Gouveia (2019), de forma similar, resume tal termo como sendo a proteção da informação, dos sistemas e dos dispositivos que a permeiam.

2.1.1 Princípios de segurança da informação

A informação tem se tornado um ativo cada vez mais crucial em todas as organizações, sejam elas públicas ou privadas. Com sua crescente importância, o valor da segurança da informação também aumenta de forma exponencial.

Figura 1 – Pilares da segurança da informação.



Fonte – elaborada pelos autores.

À medida que a importância desse ativo cresce, novas ameaças são constantemente desenvolvidas, tornando crucial a evolução e a adaptabilidade da área de segurança da informação.

Para melhor gerenciar essa área, foi criado um conjunto de pilares fundamentais para nortear sua implementação. Esses pilares são conhecidos como a tríade CIA (*Confidentiality, Integrity, Availability*) ou, em português, simplesmente CID, correspondendo respectivamente aos critérios de Confidencialidade, Integridade e Disponibilidade.

2.1.1.1 Confidencialidade

O princípio da confidencialidade está relacionado à proteção contra acessos não autorizados, permitindo que apenas indivíduos ou sistemas autorizados tenham acesso às informações. Esse princípio pode ser aplicado de diversas formas, como por meio da autenticação ou da criptografia de dados.

2.1.1.2 Integridade

A integridade refere-se à capacidade de garantir que os dados permaneçam consistentes durante todo o seu ciclo de vida, assegurando que estejam completos e não alterados. Danos a esses dados podem causar perda de confiabilidade. Exemplos de sua aplicação incluem o uso de assinaturas eletrônicas e controle de versões.

2.1.1.3 Disponibilidade

A disponibilidade diz respeito à capacidade de garantir que a informação esteja acessível sempre que for necessária. Isso envolve verificações periódicas de software e hardware para manter sua disponibilidade. Exemplos incluem medidas contra ataques DDoS e a implementação de sistemas de redundância.

2.1.2 Principios adicionais

Além dos princípios supracitados, os princípios de segurança da informação, como autenticidade e não repúdio, desempenham um papel fundamental no contexto do Sistema de Gestão de Segurança da Informação (SGSI), conforme estabelecido em normativas como a família ISO 27001 que define um SGSI como uma abordagem sistemática para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação de uma organização. Um SGSI, de forma abrangente, trata das tecnologias, pessoas e processos, rompendo com o pensamento tradicional de que a segurança da informação se restringe apenas à parte cibernética, como antivírus e firewalls. Este sistema permite que todas as medidas de segurança cibernética, física e de processos se integrem de forma dinâmica e coerente, resultando em meios robustos de segurança. Exemplos desses métodos são o CIS Controls V8, ISO 2700 e NIST.

A autenticidade, que garante a veracidade de uma identidade ou documento, é um princípio essencial para a confiança nos processos de comunicação e transações digitais. Técnicas como assinaturas digitais e certificados digitais são comumente utilizadas para assegurar que as partes envolvidas em uma transação ou interação sejam devidamente identificadas e que a informação não tenha sido alterada.

Por outro lado, o princípio do não repúdio assegura que o autor de uma ação, como a criação ou assinatura de um documento, não possa negar sua responsabilidade. Esse princípio reforça a integridade e a confidencialidade da informação, fornecendo uma camada adicional de segurança e transparência nas interações. Juntos, esses princípios não apenas ampliam a robustez dos sistemas de segurança, mas também possibilitam a conformidade com regulamentações legais e exigências regulatórias, como aquelas previstas por legislações nacionais.

Integrados a um SGSI, esses princípios garantem que a segurança da informação seja tratada de forma holística, incluindo aspectos tecnológicos, humanos e processuais, em vez de se restringir apenas à proteção cibernética. A implementação desses princípios fortalece a adaptabilidade dos sistemas de informação, permitindo sua aplicação em diferentes contextos e a

implementação de controles eficazes para proteger dados sensíveis e garantir a continuidade dos negócios.

2.2 Modelos e controles de segurança da informação

Nesta seção, serão explorados os controles normatizados por organizações como a ISO, NIST e CIS, que fornecem frameworks amplamente reconhecidos para garantir a proteção dos dados e a continuidade dos processos organizacionais.

O objetivo é apresentar as melhores práticas e abordagens para garantir a segurança dos sistemas de informação, permitindo uma gestão eficiente dos riscos e a conformidade com requisitos regulatórios.

2.2.1 CIS Controls V8

Lançado em 18 de maio de 2021, o *CIS Controls* é um conjunto de publicações que apresenta boas práticas e recomendações para a área de segurança da informação. Esses controles de salvaguardas foram criados com o objetivo de prevenir e mitigar ataques cibernéticos. Um fato interessante sobre o *CIS Controls* é que, à medida que os meios tecnológicos evoluem, ele se aperfeiçoa para acompanhar essas mudanças. Para melhor compreensão, o framework *CIS Controls* é dividido em 18 controles diferentes, que são apresentados no quadro a seguir.

Quadro 1 – Controles do CIS Controls V8

Controle	Descrição
C1. INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS	Estabelece a necessidade de um inventário de todos os dispositivos, móveis ou fixos, na organização, facilitando a proteção de ativos importantes e a identificação de infiltrações de agentes não autorizados.
C2. INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE	Semelhante ao controle C1, este dispositivo visa identificar e classificar os softwares em execução no ambiente, permitindo uma gestão e controle mais seguros.
C3. PROTEÇÃO DE DADOS	Estabelece controles e métricas técnicas para gerenciar o ciclo de vida dos dados, desde sua criação até armazenamento, classificação e destruição.
C4. CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE	Este controle recomenda a criação de processos e procedimentos para proteger os ativos institucionais e garantir a configuração segura de software.

C5. GESTÃO DE CONTAS	O objetivo principal desse controle é reduzir o risco de acesso não autorizado aos sistemas e dados da organização, garantindo que apenas as pessoas certas, com os direitos de acesso apropriados, possam interagir com os recursos críticos. Além disso, ajuda a minimizar os impactos de erros humanos, como a criação de contas de usuário desnecessárias ou a manutenção de contas inativas, que podem ser exploradas por agentes mal-intencionados.
C6. GESTÃO DO CONTROLE DE ACESSO	Complementa o controle anterior, cuidando da criação, manutenção, atribuição e revogação do grau de acesso concedido aos indivíduos.
C7. GESTÃO CONTÍNUA DE VULNERABILIDADES	Estabelece que se deve criar um plano para verificar periodicamente possíveis vulnerabilidades.
C8. GERENCIAMENTO DE LOGS DE AUDITORIA	Define a necessidade de coletar, analisar e reter arquivos de auditoria de eventos, com o intuito de descobrir, prevenir e estudar possíveis ataques.
C9. PROTEÇÕES DE NAVEGADORES WEB E E-MAIL	Este controle foca em estratégias para proteger dois dos principais vetores de ataque utilizados por cibercriminosos: e-mail e navegadores web. Esses canais são frequentemente explorados para a disseminação de malware, phishing e outras ameaças cibernéticas. A implementação eficaz de proteções nestes pontos ajuda a mitigar os riscos associados a ataques cibernéticos.
C10. DEFESAS CONTRA MALWARE	Busca prevenir que scripts maliciosos infectem ou ataquem a infraestrutura da empresa. Este controle se concentra na implementação de medidas e práticas para proteger os sistemas e redes contra ataques de malware, como vírus, ransomware, spyware, trojans e outros tipos de software malicioso. O objetivo principal deste controle é minimizar a probabilidade de infecção por malware e reduzir o impacto caso ocorra uma violação de segurança.

C11. RECUPERAÇÃO DE DADOS	Este controle trata da importância de garantir que os dados e sistemas críticos possam ser recuperados de forma eficaz após um incidente de segurança, como um ataque de ransomware , falha de hardware ou outro tipo de desastre. A recuperação de dados é uma parte fundamental de qualquer estratégia de segurança cibernética, pois permite que uma organização se recupere rapidamente e minimize o impacto de incidentes que podem afetar a integridade e disponibilidade dos dados.
C12. GERENCIAMENTO DA INFRAESTRUTURA DE REDE	Este controle tem como objetivo garantir que a infraestrutura de rede de uma instituição seja configurada, monitorada e mantida de forma segura, minimizando as vulnerabilidades e os riscos associados à rede. Ele visa melhorar a segurança da rede, protegendo os sistemas, dados e dispositivos que estão interconectados, e evitando o acesso não autorizado ou a exploração de falhas.
C13. MONITORAMENTO E PROTEÇÃO DA REDE	O principal objetivo deste controle é monitorar a rede em tempo real para identificar ameaças e incidentes de segurança, além de proteger a rede com mecanismos que garantem sua integridade e que impedem ou mitigam ataques e acessos não autorizados. O controle envolve tanto a implementação de ferramentas de segurança, como firewalls e sistemas de detecção de intrusões, quanto a análise contínua do tráfego da rede e a correlação de eventos de segurança.
C14. TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA	Este controle foca na importância de garantir que os funcionários, colaboradores e usuários de uma organização tenham o conhecimento e a conscientização necessários sobre os riscos de segurança cibernética e as melhores práticas para proteger a informação e os sistemas da organização. Muitas violações de segurança ocorrem devido a erros humanos, como clicar em links maliciosos ou falhar em seguir protocolos de segurança. Por isso, a educação e o treinamento contínuo são cruciais para reduzir esses riscos.

C15. GESTÃO DE PRESTADORES DE SERVIÇO	Aborda a importância de gerenciar e proteger os relacionamentos com prestadores de serviços externos, como fornecedores, contratados ou parceiros comerciais, que têm acesso aos sistemas e dados da organização. Muitas vezes, esses prestadores de serviços têm acesso direto ou indireto a informações confidenciais ou à infraestrutura de TI, o que pode representar riscos significativos para a segurança. Portanto, garantir que esses terceiros sigam as mesmas práticas de segurança que a organização é fundamental para proteger as informações e a continuidade dos negócios.
C16. SEGURANÇA DE APLICAÇÕES	Este controle aborda as práticas e estratégias essenciais para garantir que as aplicações utilizadas pela organização sejam seguras contra ameaças cibernéticas.
C17. GESTÃO DE RESPOSTA A INCIDENTES	Trata da criação e implementação de um plano estruturado para lidar com incidentes de segurança, de modo a minimizar os impactos sobre a organização, suas operações e dados. Incidentes de segurança podem ocorrer a qualquer momento e, caso não sejam tratados de forma eficaz, podem resultar em danos significativos, como perda de dados, interrupção de serviços, roubo de informações confidenciais ou danos à reputação da organização. Portanto, a resposta rápida e bem coordenada é essencial para mitigar esses riscos.
C18. TESTE DE INVASÃO	Busca avaliar a eficácia das medidas de proteção por meio de testes de penetração periódicos, simulando os métodos de possíveis invasores.

Fonte – Elaborado pelos autores.

Os *CIS Controls* são um dos frameworks de segurança da informação mais adotados e cobrem as principais bases da LGPD (Lei Geral de Proteção de Dados Pessoais). Embora a documentação os descreve como um “conjunto de boas práticas”, eles mostram uma abordagem robusta para implementar e aprimorar os sistemas de segurança. Sua flexibilidade e versatilidade permitem que sejam aplicados em diversos ambientes e áreas, mantendo sempre um padrão de qualidade elevado.

No *CIS Controls*, cada um dos 18 controles do quadro acima possui um conjunto de medidas associadas. Esta divisão é feita de forma estratégica para garantir uma abordagem organizada e prática na implementação de segurança cibernética. A ideia de dividir os controles

em medidas específicas no *CIS Controls* é criar uma estrutura prática que permita às instituições implementarem segurança de forma incremental, com foco naquilo que é mais crítico e vulnerável. Isso torna a gestão de segurança mais acessível, especialmente para empresas com recursos limitados.

As medidas que compõem cada controle são orientadas para a aplicação de práticas comprovadas e escaláveis, que podem ser adaptadas conforme a evolução das ameaças e a maturidade da organização. Essa abordagem modular também facilita a priorização de ações, uma vez que cada medida ou conjunto de medidas representa uma intervenção prática para mitigar riscos reais e comuns enfrentados pelas organizações no ambiente digital.

2.2.2 ISO 27000

A *International Organization for Standardization* (ISO), criada em 1947, é caracterizada por ser uma organização não governamental e independente que busca criar normas, testes e certificações para facilitar o comércio e as relações em diversos países, contando atualmente com 148 países membros. Um exemplo prático disso é o plugue de tomada, o qual é normatizado para evitar que diferentes fabricantes desenvolvam seus próprios modelos, inviabilizando o uso de um produto em diferentes locais.

Dito isso, a ISO 27000 segue a mesma vertente, sendo um conjunto de certificações que visam viabilizar a criação de um Sistema de Gestão de Segurança da Informação (SGSI). Essa norma foi criada em parceria com a International Electrotechnical Commission (IEC), voltada para a normalização de itens relacionados à eletricidade e eletrônica. Sua aplicação pode ocorrer em diversos meios, abrangendo empresas de pequeno, médio e grande porte. A versão mais recente apresenta alguns princípios norteadores da segurança da informação, que incluem: integridade, disponibilidade, confidencialidade e autenticidade.

A família de normas ISO 27000 abrange diversos padrões relacionados à segurança da informação, entre os quais se destacam três principais: ISO 27001, ISO 27002 e ISO 27005. A norma ISO 27001 estabelece os requisitos para a criação, manutenção e aprimoramento contínuo de um Sistema de Gestão de Segurança da Informação (SGSI). Seu objetivo é garantir a proteção das informações por meio da identificação de ameaças e da prevenção de possíveis incidentes.

Um diferencial importante da ISO 27001 é a possibilidade de certificação, permitindo que organizações demonstrem a conformidade com seus requisitos e assegurem a terceiros a robustez de sua segurança da informação. A adoção dessa norma proporciona benefícios como maior credibilidade da marca, redução de custos com incidentes futuros e alinhamento com exigências legais.

A segunda norma que mencionaremos aqui, a ISO 27002, é utilizada frequentemente em conjunto com a ISO 27001. Essa norma atua como um código de boas práticas, oferecendo diretrizes para a implementação eficaz de um SGSI. Ela descreve as melhores práticas para gerenciar tecnologias, processos e pessoas, porém, diferentemente da ISO 27001, não permite certificação. A ISO 27002 é estruturada em 93 controles organizados nas quatro categorias

descritas no quadro a seguir.

Quadro 1 – Controles do CIS Controls V8

Categoria e controles	Descrição
PESSOAIS (8)	Essa categoria inclui 8 controles voltados para a segurança das pessoas dentro da organização, visando minimizar riscos relacionados ao fator humano. Isso envolve desde a conscientização dos colaboradores até processos de contratação e desligamento. Alguns exemplos de controles dessa categoria incluem: • Educação e conscientização em segurança da informação – Treinamentos para funcionários sobre boas práticas e ameaças cibernéticas. • Política de controle de acessos baseados em identidade – Regras para conceder, revisar e revogar acessos a informações e sistemas. • Gestão de credenciais – Definição de padrões seguros para senhas e autenticação de usuários.
FÍSICOS (14)	Os controles físicos protegem ativos tangíveis da organização, como servidores, escritórios e data centers, contra acessos não autorizados, danos ou roubos. Exemplos incluem: • Controle de acesso a áreas restritas – Uso de cartões de acesso, biometria e monitoramento para limitar a entrada em locais sensíveis. • Proteção contra desastres naturais e incêndios – Implementação de medidas como alarmes, extintores e redundância na infraestrutura. • Gestão de dispositivos e mídia removível – Definição de regras para armazenamento e descarte seguro de equipamentos, como pendrives ou discos rígidos. de padrões seguros para senhas e autenticação de usuários.

ORGANIZACIONAIS (37)	Essa categoria abrange controles relacionados à governança da segurança da informação, garantindo que políticas e processos estejam alinhados às estratégias da organização. Alguns controles dessa categoria incluem: • Definição de papeis e responsabilidades – Especificação das funções e deveres de cada colaborador em relação à segurança da informação. • Gestão de riscos de segurança da informação – Avaliação e mitigação de ameaças, considerando os impactos nos negócios. • Planos de resposta a incidentes – Procedimentos para detectar, responder e recuperar-se de incidentes de segurança. de padrões seguros para senhas e autenticação de usuários.
TECNOLÓGICOS (34)	Os controles tecnológicos abordam a proteção de sistemas, redes e dados contra ataques e falhas de segurança. Exemplos desse controles incluem: • Gerenciamento de vulnerabilidades e atualizações – Aplicação de patches e correções para mitigar riscos cibernéticos. • Proteção contra malware – Uso de antivírus, firewalls e outras soluções de segurança. • Criptografia e proteção de dados – Implementação de técnicas de criptografia para garantir a confidencialidade das informações.

Fonte – Elaborado pelos autores.

A última norma ISO de segurança da informação abordada nesse trabalho é a ISO 27005, que se concentra na gestão de riscos da segurança da informação, sendo fundamental para a identificação, avaliação e tratamento de ameaças. Aplicável a organizações de diferentes portes e setores, essa norma segue um processo interativo composto por três etapas principais:

- Identificação de riscos – Levantamento e categorização dos fatores de risco, gerando uma

lista de ameaças potenciais.

- Análise de riscos – Avaliação da relevância e do impacto dos riscos, conforme critérios previamente definidos.
- Avaliação de riscos – Priorização dos riscos analisados para determinar as ações de tratamento mais adequadas.

Ao final dessas etapas, se a avaliação for satisfatória, passará para a etapa de tratamento; caso contrário, retornará ao fluxo anterior. Na etapa de tratamento, se o tratamento for aceito, o objeto em questão passará a ser monitorado e revisado; caso contrário, também retornará ao fluxo.

2.2.3 NIST

O *National Institute of Standards and Technology* (NIST) é uma agência governamental não reguladora da administração de tecnologia do Departamento de Comércio dos Estados Unidos, que promove a inovação e competitividade por meio do estabelecimento de padrões para fomentar o meio econômico. Esse instituto criou o *NIST Cybersecurity Framework*, que oferece um conjunto abrangente de melhores práticas e orientações com o objetivo de melhorar a segurança da informação e a gestão de riscos cibernéticos, proporcionando a entidades dos setores público e privado formas de prevenir, detectar e responder a ataques cibernéticos.

De forma geral, o NIST organiza seu *framework* em funções, categorias, subcategorias e referências informativas. As funções contêm informações gerais sobre os protocolos e boas práticas a serem implementadas, enquanto as categorias e subcategorias apresentam os planos de ação a serem executados. Existem 5 funções e um total de 23 categorias, sendo elas:

1. **Identificar**: esta função visa identificar todos os ativos organizacionais para melhor gerenciá-los e mantê-los sob controle e proteção. Algumas categorias que fazem parte desta função são: governança, avaliação de riscos e gestão de ativos.
2. **Proteger**: esta função tem como objetivo implementar medidas voltadas à proteção de ativos críticos para a organização e à identificação de possíveis ameaças. Nesta função, encontram-se categorias como: segurança de dados, monitoramento contínuo de ameaças e conscientização e treinamento.
3. **Detectar**: esta função visa implementar medidas que alertem sobre a ocorrência de um possível ataque cibernético, possuindo categorias como: anomalias e eventos, processos de detecção e monitoramento contínuo de ameaças.
4. **Responder**: esta função tem como finalidade garantir um grau de resposta adequado a ataques e violações cibernéticas, com categorias como: análise, mitigação e melhorias.

5. **Recuperar**: esta função visa garantir meios de recuperação diante de diversas ocorrências, assegurando o funcionamento ou a recuperação do sistema. As categorias dessa função incluem: planejamento de recuperação, melhorias e recuperação.

De forma geral, o NIST oferece um passo a passo para implementar ou aprimorar um sistema de gestão de riscos, que inclui:

1. **Priorizar e definir escopo**: Esta etapa envolve a criação de critérios para priorizar o que deve ser abordado e em que escopo o sistema estará estruturado, estabelecendo a tolerância a riscos da organização.

2. **Orientar**: Consiste em fazer um inventário dos ativos da organização, definindo a melhor abordagem ao risco e identificando os possíveis riscos a que está exposta.

3. **Criar um perfil atual**: Visa criar um perfil de como a organização está lidando atualmente com a gestão de riscos, seguindo os critérios do NIST.

4. **Conduzir uma avaliação de risco**: Nesta etapa, é feito um balanço geral sobre o ambiente da organização, riscos emergentes e informações sobre ataques cibernéticos, com o propósito de identificar a probabilidade e o impacto de um ataque.

5. **Criar um perfil de destino**: Envolve desenvolver um perfil modelo que a organização busca alcançar.

6. **Determinar, analisar e preencher lacunas**: Trata-se de estabelecer um paralelo entre o perfil atual e o perfil de destino, identificando marcos alcançáveis e deficiências que precisam ser corrigidas.

7. **Implementar plano de ação**: refere-se à execução do plano

2.3 Segurança da informação na Administração Pública Federal

Esta seção discute sobre a segurança da informação na administração pública federal, explorando em detalhes a Política Nacional de Segurança da Informação (PNSI) e o Programa de Privacidade e Segurança da Informação (PPSI). A PNSI estabelece diretrizes amplas para a proteção das informações estratégicas do país, garantindo a confidencialidade, integridade e disponibilidade dos dados governamentais. Complementarmente, o PPSI específica normas e procedimentos voltados para os órgãos e entidades da administração pública federal, assegurando a implementação eficaz das diretrizes estabelecidas pela PNSI no contexto governamental.

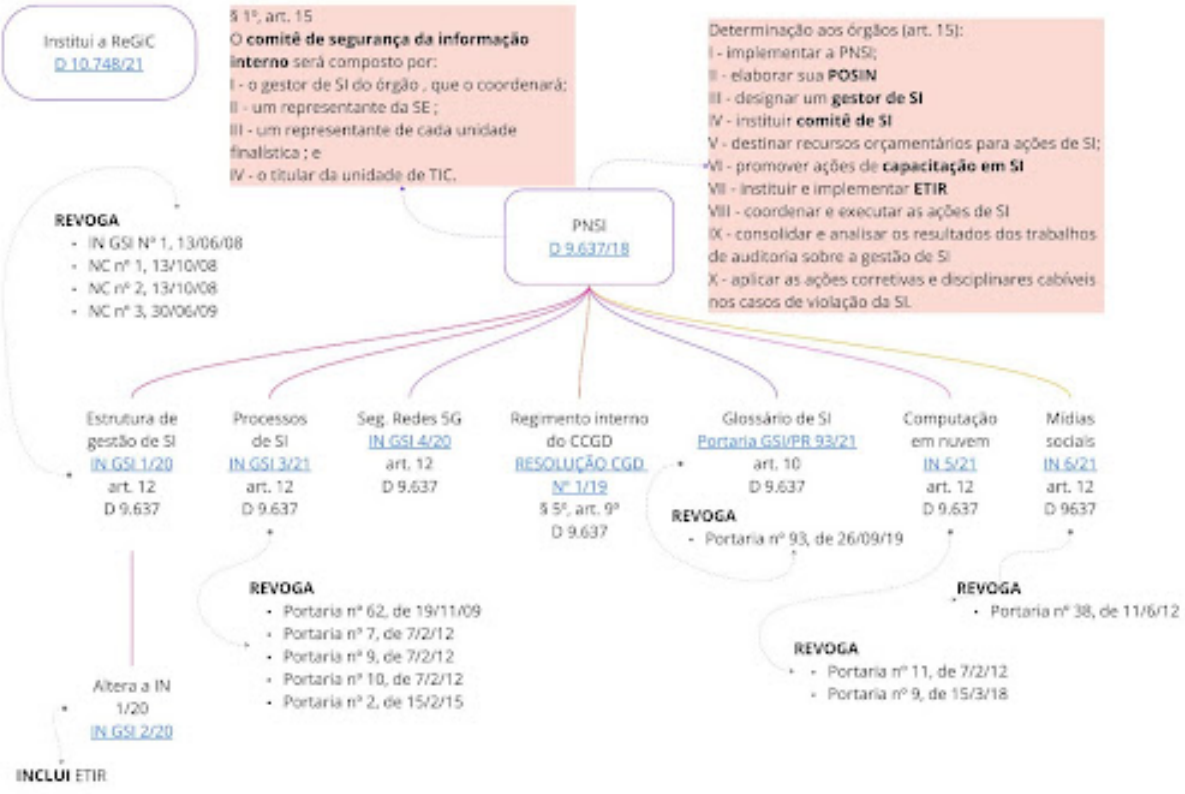
2.3.1 PNSI

O Decreto nº 9.637, de 26 de dezembro de 2018 instituiu, no âmbito da administração pública federal, a Política Nacional de Segurança da Informação (PNSI), com o objetivo de

assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações estratégicas do país.

O referido normativo estabelece diretrizes e princípios fundamentais para garantir a segurança da informação, promovendo ações coordenadas entre órgãos governamentais e demais setores da sociedade. Na Figura 2, é possível visualizar um resumo esquemático do Decreto nº 9.637/2018 e a relação com os documentos publicados pelo GSI, que complementam sua implementação. Essa estrutura normativa garante que as políticas de segurança da informação sejam aplicadas de maneira uniforme e eficiente em toda a administração pública federal.

Figura 2 – resumo esquemático do Decreto 9.637/2018 e documentos complementares.



Fonte – elaborada pelos autores.

A PNSI se baseia em diversos princípios, incluindo:

- soberania nacional, garantindo que o Brasil tenha autonomia na gestão de suas informações estratégicas;
- respeito aos direitos fundamentais, abrangendo a proteção de dados pessoais, privacidade e liberdade de expressão;
- visão sistêmica da segurança da informação, integrando diferentes abordagens para fortalecer a proteção de dados;
- educação e conscientização, promovendo uma cultura de segurança da informação dentro da administração pública e na sociedade; e

- gestão de riscos e prevenção de incidentes, permitindo a identificação e mitigação de ameaças de forma proativa.

A PNSI tem como objetivo fortalecer a segurança da informação em diferentes esferas do governo e da sociedade, promovendo:

- a proteção de infraestruturas críticas e informações sensíveis;
- a pesquisa e inovação em tecnologias de segurança;
- a cooperação internacional para aprimorar mecanismos de defesa cibernética; e
- o desenvolvimento de normativas que regulamentam a segurança da informação no país.

Como instrumentos de implementação, para garantir a efetividade da PNSI, o decreto estabelece a Estratégia Nacional de Segurança da Informação e planos nacionais específicos que detalham ações e metas para sua implementação. Além disso, o Gabinete de Segurança Institucional (GSI) da Presidência da República desempenha um papel central na coordenação dessas iniciativas, supervisionando a aplicação das diretrizes e emitindo documentos complementares que aprofundam a regulamentação da política. Estes documentos estabelecem normas técnicas e operacionais, fornecendo diretrizes mais específicas para a proteção de dados governamentais.

O Decreto nº 9.637/2018 representa um avanço significativo na governança da segurança da informação no Brasil. Ao estabelecer diretrizes claras e mecanismos de implementação, a política contribui para o fortalecimento da segurança da informação e da proteção de dados sensíveis e reforça a soberania nacional frente às ameaças cibernéticas.

2.3.2 PPSI

O Programa de Privacidade e Segurança da Informação (PPSI), formalizado por meio da Portaria SGD/MGI nº 852, de 28 de março de 2023, é uma iniciativa do governo brasileiro para garantir a proteção das informações, no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação[4] (SISP).

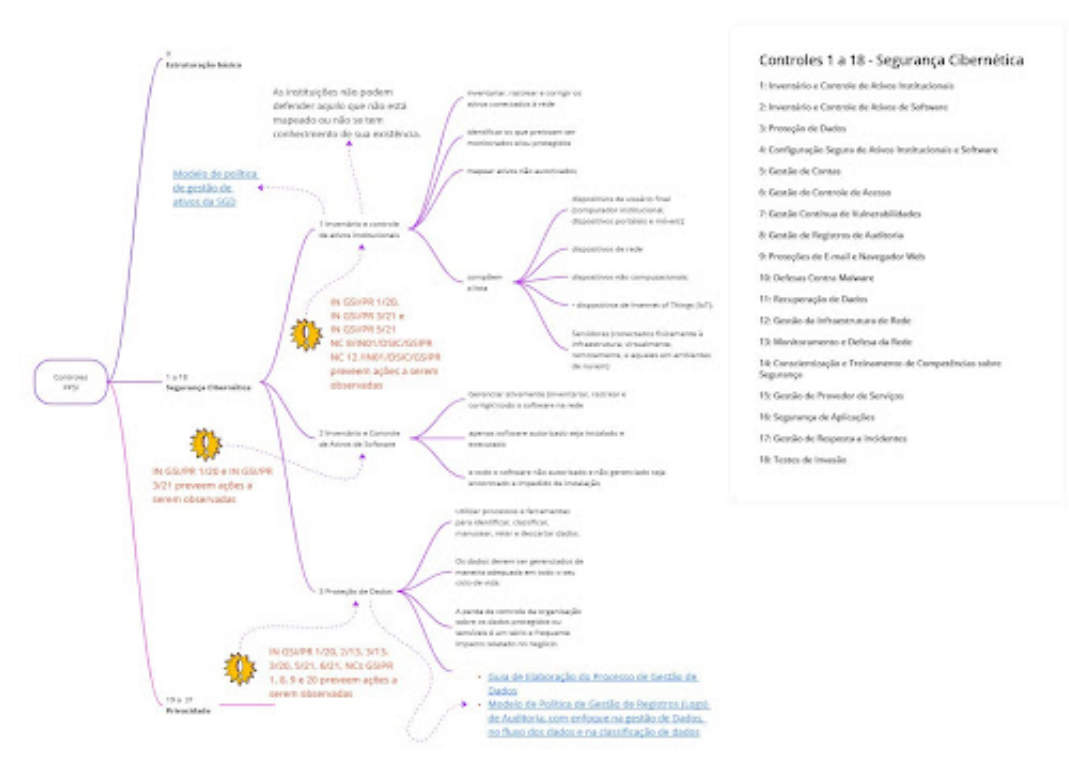
O principal objetivo do programa é assegurar a confidencialidade, integridade e disponibilidade dos ativos informacionais dos órgãos públicos, reduzindo riscos relacionados a vazamentos, acessos não autorizados e indisponibilidade de sistemas críticos.

No âmbito do PPSI, nasce o Framework de Privacidade e Segurança da Informação como uma iniciativa que propõe ações concretas para auxiliar as instituições públicas na identificação, acompanhamento e preenchimento de lacunas existentes em suas práticas de privacidade e segurança da informação.

[4] O Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) foi instituído pelo Decreto nº 7.579/2011 e tem como objetivo coordenar e orientar a gestão da tecnologia da informação na Administração Pública Federal, garantindo a padronização, eficiência e segurança dos sistemas governamentais.

O framework disponibiliza uma série de guias, modelos e ferramentas que auxiliam na aplicação prática das diretrizes propostas, facilitando a adaptação das instituições às melhores práticas e normas internacionais.

Figura 3 – controles do Framework do PPSI.



Fonte – elaborada pelos autores.

O framework do PPSI é composto de um conjunto de medidas de 32 controles em 3 grandes categorias, a saber: controle de estrutura básica de governança (controle 0), controle de cibersegurança (controles 1 a 18) e controles de privacidade (controles 19 a 31), conforme ilustrado na Figura 3.

O controle da estrutura básica de governança do framework do PPSI serve principalmente para estabelecer papéis e responsabilidades, garantindo que uma estruturação básica em segurança da informação e privacidade seja estabelecida no órgão ou entidade. Assim, esse controle, contendo 7 medidas , busca garantir que a segurança da informação seja tratada como uma questão organizacional, alinhada aos objetivos institucionais e normativas vigentes.

Os controles do framework do PPSI relativo à segurança cibernética, controle 1 a 18, são baseados nos Controles de Cibersegurança do *Center for Internet Security* (CIS) versão 8 e abrangem diversas áreas essenciais para a proteção da informação. Cada um desses controles é composto por diversas medidas específicas que detalham as ações necessárias para sua implementação. O número de medidas varia conforme a complexidade de cada controle, totalizando 153 medidas relacionadas à segurança cibernética. O Guia do Framework de Privacidade e Segurança da Informação detalha cada controle e suas respectivas medidas. Os controles do framework

relacionados à privacidade, por sua vez, são os controles 19 a 31, complementando os controles anteriores que tratam da cibersegurança. Esses controles visam assegurar que as instituições públicas tratem os dados pessoais de forma responsável e em conformidade com a legislação vigente, protegendo os direitos dos titulares e garantindo a integridade e confidencialidade das informações. Neste grupo de controles encontram-se 151 medidas de privacidade.

O framework do PPSI estabelece conjuntos de medidas prioritárias, organizadas em ciclos. Cada ciclo é planejado para ocorrer ao longo de um semestre, com a exigência de que todas as medidas priorizadas para aquele ciclo sejam implementadas pelos órgãos até o final de cada período. O primeiro ciclo contemplava 41 medidas a serem implementadas até dezembro de 2023, o segundo ciclo prevê a implementação de 30 medidas até junho de 2024, e o terceiro ciclo inclui 25 medidas com prazo até dezembro de 2024. O ciclo atual estabelece 33 medidas a serem implementadas até junho de 2025. Além disso, ainda estão previstas medidas para os ciclos 5, 6 e 7, com prazos de implementação em dezembro de 2025, junho de 2026 e dezembro de 2026, totalizando 310 medidas planejadas no framework.

Percebe-se que o framework do PPSI é essencial para a administração pública federal, pois estabelece um rol de ações concretas para garantir a proteção dos dados e informações sensíveis, que são vitais para a segurança do Estado e a privacidade dos cidadãos. Ele assegura a conformidade com normas e regulamentações, como a Lei Geral de Proteção de Dados (LGPD), e facilita a gestão de riscos, mitigando ameaças como ataques cibernéticos e vazamentos de dados. Além disso, a implementação do PPSI fortalece a confiança pública nas instituições governamentais, demonstrando um compromisso com a segurança da informação, e promove maior eficiência operacional ao estruturar as ações de proteção e governança da TI nos órgãos federais.

3 TRABALHOS RELACIONADOS

Diversos estudos propõem metodologias e modelos para aprimorar a tomada de decisão e o monitoramento de estratégias de segurança da informação. Nesta seção, apresentamos os principais trabalhos relacionados a esta pesquisa, destacando suas contribuições no contexto da segurança da informação e da gestão pública em setores da educação, saúde e financeiro.

3.1 A Review of Cybersecurity Management Standards Applied in Higher Education Institutions (Uma Revisão dos Padrões de Gestão de Cibersegurança Aplicados em Instituições de Ensino Superior)

Neste trabalho, Amine et al. (2023) analisam os padrões de gestão de cibersegurança em instituições de ensino superior, destacando a importância da adoção das normas ISO/IEC 27001 e do NIST Cybersecurity Framework (CSF) para mitigar riscos e fortalecer a segurança da informação.

Os autores avaliam os pontos em comum entre as duas abordagens destacando que ambas utilizam uma estratégia de implementação de segurança baseada em recomendações e

gerenciamento de riscos. Os controles e salvaguardas de segurança são implementados apenas quando os riscos identificados são considerados inaceitáveis, servindo como referência para monitorar o progresso contínuo.

Além disso, há pontos chaves de semelhança a serem considerados. O primeiro é o fato de que ambos podem ser aplicados em quaisquer setores e organizações; já o segundo se refere ao que os autores chamam de neutralidade tecnológica, uma vez que tanto o NIST-CSF quanto o ISO/IEC 27001 são construídos com base em princípios gerais de segurança, permitindo que as organizações escolham as tecnologias mais adequadas e ecologicamente corretas.

Amine et al. (2023) também verificaram as distinções entre o NIST-CSF e o ISO/IEC 27001, evidenciando que a estrutura do NIST-CSF concentra-se no planejamento e implementação da segurança cibernética, enquanto a ISO/IEC 27001 aborda o assunto de forma mais abrangente. Sua metodologia baseada em PDCA (Plan, Do, Check, Act) não apenas executa o sistema como também garante sua manutenção durante uma auditoria.

Os autores concluem que em vez de escolher uma das duas abordagens, o melhor é combiná-las. O NIST-CSF é mais eficaz na organização dos domínios de segurança a serem implementados, enquanto o ISO/IEC 27001 se destaca em governar e criar um sistema de gerenciamento de segurança de informações sustentável.

3.2 Proposta de avaliação da Política Nacional de Segurança da Informação por Processo de Análise Hierárquica

Gavião et al. (2022) avaliam a Política Nacional de Segurança da Informação (PNSI) por meio do Processo de Análise Hierárquica (AHP) aplicado ao NIST-CSF, com o objetivo de aprimorar a análise e a tomada de decisões sobre as ações de segurança.

Segundo Gavião et al. (2022), O CSF-NIST é aplicável aos setores público ou privado, devido ao seu caráter customizável, focado na melhoria da segurança e resiliência para cada organização. Além disso, o modelo apresenta aderência aos marcos regulatórios nacionais, pois atende às necessidades mencionadas no Art. 12 da PNSI, de competência do GSI, referentes ao Inciso VII. De igual forma, é possível relacionar aspectos do modelo ao Art. 17, de competência dos órgãos e entidades da APF, nos Incisos II, VII e VIII.

O AHP é um método de apoio à decisão multicritério que estrutura problemas complexos em uma hierarquia de critérios e subcritérios, permitindo comparações ponderadas entre alternativas. O método funciona estruturando problemas complexos em níveis hierárquicos, organizando o objetivo principal no topo, seguido por critérios, subcritérios e alternativas de decisão. As comparações entre os elementos são feitas de forma paritária, utilizando uma escala numérica de importância relativa. A partir dessas comparações, são calculados pesos para cada critério, permitindo priorizar alternativas com base em fatores quantitativos e qualitativos.

Com isso, Gavião et. al (2022) desenvolvem um estudo de caso aplicado a um banco público onde o método AHP é utilizado para definir os pesos de cada critério de segurança que serão tratados pelo CSF-NIST. Concluindo que o CSF-NIST é o modelo conceitual que

melhor se adequa no atendimento das necessidades estabelecidas pelo Decreto No 9.637 e que a aplicação do AHP proporciona uma avaliação mais objetiva e estruturada.

3.3 Manual de boas praticas de seguranca da informacao para os sistemas de telemedicina tendo como base a norma ABNT NBR ISO/IEC 27002 e o framework CIS Controls

O trabalho de Querido (2023) propõe um modelo estruturado para implementação e manutenção da Segurança da Informação (SI) em sistemas de telemedicina. O estudo fundamenta-se em normas técnicas amplamente aceitas, como a ISO/IEC 27001, ISO/IEC 27002 e o CIS Controls, abordando os desafios da proteção de dados em um setor crítico da saúde. A pesquisa segue uma metodologia qualitativa, exploratória e bibliográfica, analisando os processos necessários para garantir a integridade, confidencialidade e disponibilidade das informações na telemedicina.

O autor destaca que dentre as normas e frameworks de Segurança da Informação existentes no mercado e na literatura, o CIS Controls foi considerado como a principal referência para definição dos controles para garantir o atendimento às exigências identificadas, bem como a ferramenta apresenta grupos de implementação dos controles de acordo com a quantidade de recursos financeiros e exposição ao risco das organizações, de modo a ser possível identificar facilmente quais controles são mais críticos de serem implementados para obter um nível inicial de gerenciamento da segurança.

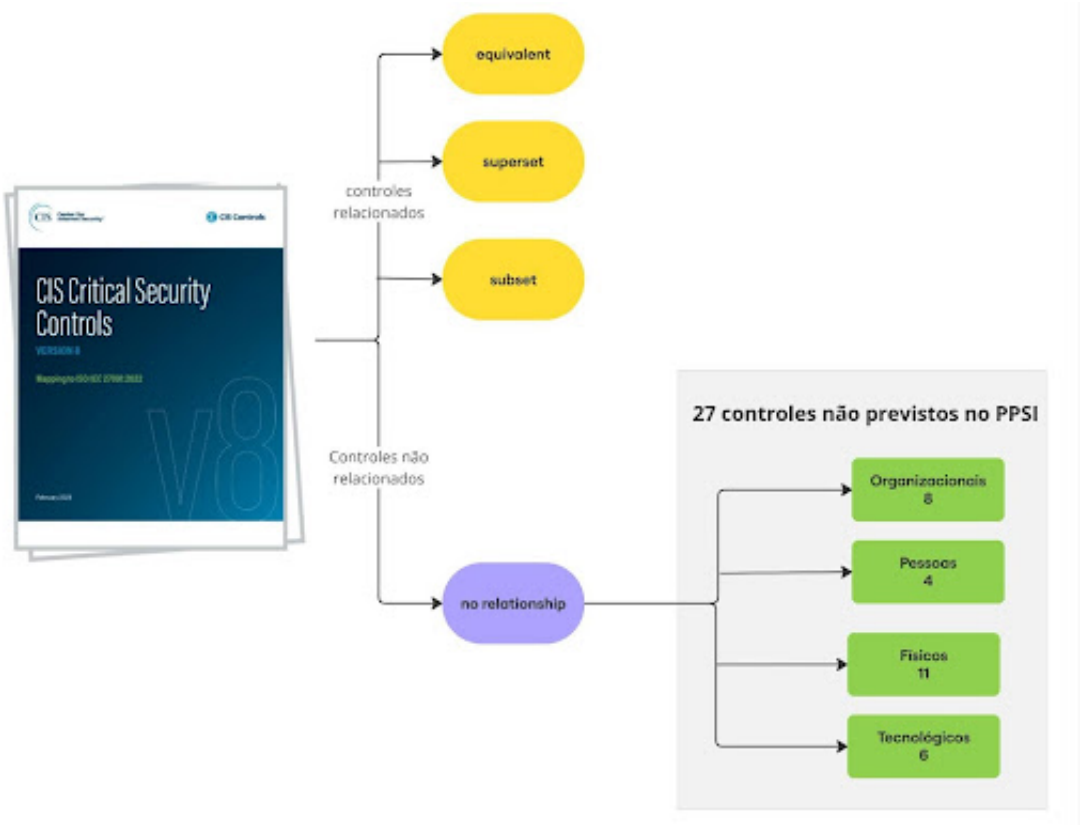
Querido (2023) conclui ressaltando que o manual é aplicável a todas as organizações do setor da saúde, independente da sua dimensão, natureza ou tipologia desde que possua sistema de telemedicina. Alerta ainda sobre a necessidade de implementação da ISO/IEC 27701 para adequação à Lei Geral de Proteção de Dados (LGPD).

Os trabalhos apresentados nesta seção evidenciam a crescente preocupação com a segurança da informação em setores como educação, saúde e administração pública, reforçando a relevância das ferramentas analisadas neste estudo. Destaca-se a necessidade de combinar e adaptar modelos para garantir a proteção eficaz dos dados. Além disso, a segurança da informação se mostra um campo multidisciplinar, demandando abordagens flexíveis e metodologias robustas para assegurar a confidencialidade, integridade e disponibilidade das informações, independentemente do contexto de aplicação.

4 METODOLOGIA

O desenvolvimento deste trabalho iniciou-se com uma pesquisa documental para compreender os modelos de segurança da informação existentes e o escopo de atuação de cada um deles. A primeira fase consistiu no estudo das principais estruturas de segurança da informação, com o objetivo de identificar suas diretrizes e abordagens para a proteção dos ativos de informação. Essa análise possibilitou uma visão panorâmica das estratégias e soluções adotadas por diferentes modelos, possibilitando a comparação de abordagens existentes.

Figura 4 – identificação de controles não previstos no framework do PPSI.



Fonte – elaborada pelos autores.

Na sequência, foi realizado um estudo detalhado sobre a proteção das instituições da administração pública federal, com foco no framework do PPSI. Nesta etapa, buscou-se entender como o PPSI se constituiu, ou seja, em quais referências de modelos existentes ele teria se fundamentado. A análise também se concentrou em identificar eventuais lacunas ou deficiências no escopo do PPSI, especialmente no que diz respeito à segurança física, um aspecto frequentemente negligenciado no contexto da segurança da informação.

Com a identificação de que o PPSI se fundamentou basicamente no CIS Controls v8, tanto nos controles de segurança cibernética quanto nos controles de privacidade, a pesquisa seguiu para um estudo sobre modelos estruturados de gestão da segurança da informação física, visto ter se apresentada como uma oportunidade melhoria do referido framework.

O objetivo foi avaliar a viabilidade de incorporar esses modelos ao PPSI para complementar sua abordagem e fornecer uma solução mais robusta e completa. Após um levantamento e análise de diferentes frameworks de segurança física, chegou-se à escolha do ISO 27002, uma norma amplamente reconhecida e aplicada em segurança da informação, que inclui diretrizes para a segurança física das instalações. Como mencionado anteriormente, a ISO 27001 estabelece o que deve ser feito para gerenciar a segurança da informação, enquanto a ISO 27002 explica como implementar os controles de segurança para atender a esses requisitos. Por esta razão, como o trabalho é feito em cima dos controles em si, a norma ISO 27002 foi usada como elemento de

comparação ao CIS Controls v8.

A comparação entre as medidas de segurança física propostas pelo ISO 27002 e as já previstas no PPSI foi realizada para identificar possíveis complementaridades e ajustes necessários. Como resultado dessa análise, foi elaborada uma lista de medidas de segurança física que podem ser incorporadas ao PPSI, visando aprimorar a proteção física das instalações e garantir uma abordagem mais holística da segurança da informação.

A comparação foi feita colocando-se lado a lado as medidas previstas no CIS Controls v8 com aquelas previstas no ISO 27002, fundamentando-se no mapeamento feito pelo próprio *Center for Internet Security* (CIS) intitulado "CIS Controls v8 Mapping to ISO/IEC 27001:2022". Na metodologia de mapeamento da CIS, cada *CIS Control* (também chamado de *CIS Safeguard*) é analisado e comparado com uma mitigação defensiva da ISO 27001, utilizando critérios específicos:

- documentação formal: deve haver um processo claramente documentado abordando o controle de acesso e alterações de direitos.
- abrangência: o processo deve cobrir todos os ativos da organização, sem segregação entre diferentes equipes.
- automação: preferencialmente, ferramentas automatizadas, como SSO (*Single Sign-On*) ou serviços de diretório, devem ser utilizadas.
- consistência: sempre que houver mudança de privilégios, o processo deve garantir que os direitos do usuário sejam gerenciados adequadamente e documentados.

Para cada controle comparado, a relação entre os *frameworks* é classificada em uma das seguintes categorias:

- *equivalent* (equivalente): o conceito de segurança abordado no CIS Control é exatamente o mesmo da mitigação defensiva na ISO 27001.
- *superset* (superconjunto): o CIS Control cobre parcialmente ou amplamente a mitigação defensiva, mas com um escopo mais amplo.
- *subset* (subconjunto): o CIS Control faz parte da mitigação defensiva, mas não cobre todo o seu escopo.
- *no relationship* (sem relação): não há correspondência direta entre o CIS Control e a mitigação defensiva na ISO 27001.

Com base no mapeamento da CIS, neste trabalho realizamos um outro mapeamento considerando como existente no framework do PPSI, todos aqueles controles do CIS Controls v8 que eram classificados como (equivalent, superset ou subset) do ISO 27001. Os demais controles foram considerados inexistentes no CIS Controls V8, consequentemente no framework do PPSI. A Figura 4 ilustra o processo de mapeamento dos controles não previstos no framework do PPSI.

A metodologia adotada para a realização deste estudo foi essencialmente qualitativa, com base em análise documental e comparativa, visando aprimorar o entendimento do cenário atual da segurança da informação no âmbito das instituições públicas federais e fornecer recomendações para o fortalecimento da segurança física dentro do modelo do PPSI.

5 RESULTADOS E DISCUSÕES

A seção anterior descreve a metodologia empregada, que envolveu um estudo documental detalhado, análise comparativa entre frameworks de segurança da informação e a aplicação de um mapeamento entre o CIS Controls v8 e o ISO 27002, com o objetivo de identificar lacunas no framework do PPSI.

A partir dos resultados obtidos, foi possível verificar que muitos dos controles previstos pelo CIS Controls v8 estavam alinhados com as diretrizes do ISO 27002, proporcionando uma base sólida para a implementação de uma abordagem mais abrangente à segurança da informação física nas instituições públicas federais. A identificação dos controles equivalentes, superconjuntos e subconjuntos entre o CIS Controls v8 e o ISO 27001 ajudou a mapear quais aspectos da segurança física estavam ausentes no PPSI e possibilitou a proposição de ajustes necessários.

Os mapeamentos dos controles presentes na ISO 27002 e ausentes no framework do PPSI foram agrupados por categorias da ISO 27002, detalhando cada uma das medidas identificadas. No Quadro 3, a seguir, estão ilustradas as 9 medidas relacionadas a controles organizacionais não identificadas no PPSI. Essas medidas incluem, por exemplo, a responsabilidade da direção, que exige que a alta gestão da organização imponha e exija a aplicação das políticas de segurança da informação por todo o pessoal, uma prática fundamental para garantir o comprometimento com a proteção da informação.

Quadro 3 – Controles ORGANIZACIONAIS do ISO 27002 não previstos no framework do PPSI

Título	**Propriedade de SI**	**Conceito de SC**	**Descrição**
5.4 Responsabilidade da direção	Iden	Identificar	Convém que a direção requeira que todo pessoal aplique a segurança da informação de acordo com a política de segurança da informação estabelecida, com as políticas específicas por tema e com os procedimentos de organização.
5.11 Devolução de ativos	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que o pessoal e outras partes interessadas, conforme apropriado, devolvam todos os ativos da organização em sua posse após a mudança ou encerramento da contratação ou acordo.

5.29 Segurança da informação durante a disrupção	Confidencialidade, Integridade, Disponibilidade	Proteger, Responder	Convém que a organização planeje como manter a segurança da informação em um nível apropriado durante a disrupção.
5.31 Requisitos legais, estatutários, regulamentares e contratuais	Disponibilidade	Identificar, Responder	Convém que os requisitos legais, estatutários, regulamentares e contratuais pertinentes à segurança da informação e à abordagem da organização para tender a esses requisitos sejam identificados, documentado e atualizados.
5.32 Direitos de propriedade intelectual	Confidencialidade, Integridade, Disponibilidade	Identificar	Convém que a organização implemente procedimentos adequados para proteger os direitos de propriedade intelectual.
5.34 Privacidade de proteção de DP	Confidencialidade, Integridade, Disponibilidade	Identificar, Proteger	Convém que a organização identifique e atenda aos requisitos relativos à preservação da privacidade e proteção de DP de acordo com as leis e regulamentos aplicáveis e requisitos contratuais.
5.35 Análise crítica independente da segurança da informação	Confidencialidade, Integridade, Disponibilidade	Identificar, Proteger	Convém que a abordagem da organização para gerenciar a segurança da informação e sua implementação, incluindo pessoas, processos e tecnologias, seja analisada criticamente de forma independente a intervalos planejados ou quando ocorrem mudanças significativas.
5.36 Conformidade com políticas, regras e normas para segurança da informação	Confidencialidade, Integridade, Disponibilidade	Identificar, Proteger	Convém que o compliance da política de segurança da informação da organização, políticas, regras e normas de temas específicos seja analisado criticamente a intervalos regulares.

5.37 Documentação dos procedimentos de operação	Confidencialidade, Integridade, Disponibilidade	Proteger, Recuperar	Convém que os procedimentos de operação dos recursos de tratamento da informação sejam documentados e disponibilizados para o pessoal que necessite deles.

Fonte – Elaborado pelos autores.

Outra medida relevante não abordada no PPSI é a devolução de ativos após a mudança ou rescisão de contratos, o que é essencial para proteger os princípios da tríade CID dos ativos da organização. Este tipo de controle ajuda a garantir que ativos críticos não sejam extraviados ou mal utilizados, especialmente quando um colaborador deixa a organização.

Além disso, a segurança da informação durante a disrupção e os requisitos legais, estatutários, regulamentares e contratuais são medidas adicionais descritas no ISO 27002 que não fazem parte do framework do PPSI. A primeira garante a segurança em situações de crise, e a segunda envolve a atualização dos requisitos legais aplicáveis.. Outras lacunas encontradas referem-se à privacidade de proteção de dados pessoais, a análise crítica independente da segurança da informação e a documentação dos procedimentos operacionais, que são práticas relevantes para garantir a conformidade contínua e a robustez das ações de segurança.

No caso dos controles de pessoas, foram identificadas 4 medidas ausentes no PPSI, conforme ilustra o Quadro 4. Um exemplo disso é o controle de seleção de candidatos, que sugere a realização de verificações de antecedentes de todos os candidatos antes de sua contratação, de forma contínua, em conformidade com as leis, regulamentos e práticas éticas aplicáveis. Essa medida é essencial para garantir que os novos colaboradores não representem riscos à confidencialidade, integridade e disponibilidade das informações que irão acessar.

QUADRO 4 - Controles de PESSOAS do ISO 27002 não previstos no framework do PPSI

Título	Propriedade de SI	Conceito de SC	Descrição
6.1 Seleção	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que as verificações de antecedentes de todos os candidatos a serem contratados sejam realizadas antes que ingressem na organização de modo contínuo, de acordo com as leis, regulamentos e ética aplicáveis e que sejam proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.

6.2 Termos e condições de contratação	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que os contratos trabalhistas declarem as responsabilidades do pessoal e da organização para a segurança da informação.
6.4 Processo disciplinar	Confidencialidade, Integridade, Disponibilidade	Proteger, Responder	Convém que um processo disciplinar seja formalizado e comunicado, para tomar ações contra o pessoal e outras partes interessadas relevantes que tenham cometido uma violação da política de segurança da informação.
6.6 Acordos de confidencialidade ou não divulgação	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que acordos de confidencialidade ou não divulgação que reflitam as necessidades da organização para a proteção das informações sejam identificados, documentados, analisados criticamente em intervalos regulares e assinados por pessoal e outras partes interessadas pertinentes.

Fonte – Elaborado pelos autores.

Além disso, o ISO 27002 aborda os termos e condições de contratação, destacando a importância de incluir responsabilidades claras de segurança da informação nos contratos de trabalho, para garantir que todos os funcionários estejam cientes das obrigações que envolvem a proteção de dados e ativos da organização desde o início de seu vínculo com a empressa.

Outro ponto relevante que o ISO 27002 aborda, mas que não está explicitamente previsto no PPSI, é a criação de um processo disciplinar formal para lidar com violação das políticas de segurança da informação. Este controle sugere que a organização tenha um mecanismo estruturado para investigar e tomar medidas corretivas contra o pessoal ou outras partes interessadas que comprometem a segurança da informação. Além disso, o ISO 27002 orienta sobre a necessidade de acordos de confidencialidade ou não divulgação, que devem ser formalizados e constantemente revisados, garantindo que todas as partes envolvidas na organização ou com acesso a informações sensíveis compreendam sua responsabilidade na proteção desses dados.

QUADRO 5 - Controles FÍSICOS do ISO 27002 não previstos no framework do PPSI

Título	Propriedade de SI	Conceito de SC	Descrição
7.2 Entrada física	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que as áreas seguras sejam protegidas por controles de entrada e pontos de acesso apropriados.
7.3 Segurança de escritórios, salas e instalações.	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que seja projetada e implementada segurança física para escritórios, salas e instalações.
7.4 Monitoramento de segurança física	Confidencialidade, Integridade, Disponibilidade	Proteger, Detectar	Convém que as instalações sejam monitoradas continuamente para acesso físico não autorizado.
7.5 Proteção contra ameaças físicas e ambientais	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que a proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não à infraestrutura, seja projetada e implementada.
7.6 Trabalho em áreas seguras	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que medidas de segurança para trabalhar em áreas seguras sejam projetadas e implementadas.
7.7 Mesa limpa e tela limpa	Confidencialidade	Proteger	Convém que regras de mesa limpa para documentos impressos e mídia de armazenamento removível e regras de tela limpa para os recursos de tratamento das informações sejam definidas e adequadamente aplicadas.
7.8 Localização e proteção de equipamentos	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que os equipamentos sejam posicionados com segurança e proteção.

7.9 Segurança de ativos fora das instalações da organização	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém proteger os ativos fora das instalações da organização.
7.11 Serviços de infraestrutura	Integridade, Disponibilidade	Proteger, Detectar	Convém que as instalações de tratamento de informações sejam protegidas contra falhas de energia e outras disrupções causadas por falhas nos serviços de infraestrutura.
7.12 Segurança do cabeamento	Confidencialidade, Disponibilidade	Proteger	Convém que os cabos que transportam energia ou dados ou que sustentam serviços de informação sejam protegidos contra interceptação, interferência ou danos.
7.13 Manutenção de equipamentos	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que os equipamentos sejam mantidos corretamente para assegurar a disponibilidade, integridade e confidencialidade da informação.

Fonte – Elaborado pelos autores.

O Quadro 5 acima apresenta a lista das 11 medidas associadas à segurança física, cuja ausência no modelo do PPSI é perceptível. O ISO 27002 fornece uma série de controles relacionados à segurança física, que são essenciais para proteger as instalações e os ativos de informação da organização, mas que não estão totalmente abordados no PPSI. Um exemplo disso é o controle de entrada física, que recomenda o uso de controles de acesso adequados para proteger áreas seguras e pontos de acesso. Essa medida é importante para evitar que pessoas não autorizadas tenham acesso a informações sensíveis, garantindo assim a confidencialidade e a integridade dos dados. Além disso, o controle de segurança de escritórios, salas e instalações propõe a implementação de medidas de segurança física, como barreiras físicas e controle de entradas, para proteger o ambiente de trabalho contra acessos indesejados e eventos que possam comprometer a disponibilidade das informações.

Outras medidas relevantes descritas no ISO 27002, mas não abordadas diretamente pelo PPSI, incluem o monitoramento de segurança física, que sugere o uso de sistemas de vigilância para detectar tentativas de acesso físico não autorizado. Essa prática é fundamental para detectar incidentes de segurança e responder rapidamente a ameaças. O controle de proteção contra ameaças físicas e ambientais também é um ponto importante, pois propõe a implementação de

soluções para proteger as instalações contra desastres naturais, incêndios e outros riscos que possam afetar a infraestrutura física, impactando a disponibilidade dos sistemas de informação. Outro controle importante é o de trabalho em áreas seguras, que define medidas de segurança para proteger o ambiente de trabalho de acessos não autorizados enquanto os funcionários estiverem presentes. Essas medidas reforçam a proteção dos ativos de informação e podem ser integradas ao PPSI para garantir uma abordagem mais robusta e eficaz à segurança física.

Além disso, o ISO 27002 também aborda controles relacionados à mesa limpa e tela limpa, que estabelecem regras para proteger informações confidenciais em documentos impressos ou dispositivos móveis, promovendo a segurança da informação em ambientes físicos de trabalho. O controle de localização e proteção de equipamentos também é essencial para garantir que os equipamentos de TI sejam posicionados de maneira segura e protegidos contra danos, o que assegura a integridade e a disponibilidade das informações. Já a segurança de ativos fora das instalações garante que os ativos da organização, como laptops e mídias removíveis, sejam adequadamente protegidos mesmo fora do ambiente organizacional.

Por fim, no Quadro 6 são elencadas as medidas de controles tecnológicos, não previstas no modelo do PPSI. Um exemplo disso é o controle de mascaramento de dados, que recomenda o uso dessa técnica para proteger informações sensíveis, especialmente em ambientes de desenvolvimento ou testes. O mascaramento de dados é uma prática essencial para garantir que informações confidenciais não sejam expostas acidentalmente a pessoas não autorizadas.

QUADRO 6 - Controles TECNOLÓGICOS do ISO 27002 não previstos no framework do PPSI

Título	Propriedade de SI	Conceito de SC	Descrição
8.11 Mascaramento de dados	Confidencialidade	Proteger	Convém que o mascaramento de dados seja usado de acordo com a política específica por tema da organização sobre controle de acesso e outros requisitos específicos por tema relacionados e requisitos de negócios, levando em consideração a legislação aplicável.
8.14 Redundância dos recursos de tratamento de informações	Disponibilidade	Proteger	Convém que os recursos de tratamento de informações sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.
8.24 Uso de criptografia	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que sejam definidas e implementadas regras para o uso efetivo da criptografia, incluindo o gerenciamento de chaves criptográficas.

8.32 Gestão de mudanças	Confidencialidade, Integridade, Disponibilidade	Proteger	Convém que mudanças nos recursos de tratamento de informações e sistemas de informação estejam, sujeitas a procedimentos de gestão de mudanças.
8.33 Informações de testes	Confidencialidade, Integridade	Proteger	Convém que as informações de teste sejam adequadamente selecionadas, protegidas e gerenciadas.
8.34 Proteção de sistemas de informação durante os testes de auditoria	Confidencialidade, Integridade	Proteger	Convém que testes de auditoria e outras atividades de garantia envolvendo a avaliação de sistemas operacionais sejam planejados e acordados entre o testador e a gestão apropriada.

Fonte – Elaborado pelos autores.

Além disso, o ISO 27002 também aborda a redundância dos recursos de tratamento de informações, sugerindo a implementação de redundâncias nos sistemas para garantir a continuidade dos serviços e a disponibilidade das informações, mesmo em caso de falhas nos recursos de infraestrutura.

Outro ponto importante abordado pelo ISO 27002 é o uso de criptografia, que deve ser cuidadosamente definido e implementado dentro da organização para proteger as informações tanto em trânsito quanto em repouso. A criptografia, juntamente com o gerenciamento de chaves criptográficas, é fundamental para preservar a confidencialidade e a integridade dos dados. O controle de gestão de mudanças também é essencial, garantindo que qualquer modificação nos sistemas ou recursos de tratamento de informações seja submetida a um processo formal de avaliação e controle. Além disso, o controle de informações de testes e a proteção de sistemas de informação durante os testes de auditoria asseguram que os dados utilizados em testes e auditorias sejam protegidos, minimizando o risco de exposição de informações sensíveis durante esses processos.

Em suma, todos esses controles apresentados nos quadros desta seção, em conjunto, contribuem para uma gestão mais eficaz da segurança da informação, oferecendo uma camada extra de proteção para as operações dos órgãos se incorporados ao framework do PPSI hoje adotado pela administração pública federal.

6 CONSIDERAÇÕES FINAIS

A segurança da informação é um conceito abrangente que envolve a proteção dos dados e sistemas de informação contra ameaças e riscos que podem comprometer sua confidencialidade, integridade e disponibilidade. Ela abrange uma série de aspectos, incluindo a segurança física, de pessoas, cibernética e organizacional. A segurança física se refere à proteção das instalações e ativos contra ameaças como roubos, incêndios e desastres naturais. A segurança de pessoas envolve práticas e controles que garantem que os indivíduos com acesso a informações sejam devidamente identificados, treinados e monitorados. Já a segurança cibernética foca na proteção contra ataques digitais, como *malware* e invasões, e a segurança organizacional envolve políticas e processos para garantir a conformidade e a governança. A integração de todas essas áreas é essencial para a criação de um ambiente seguro, especialmente nos órgãos da administração pública federal, onde a proteção de dados sensíveis é fundamental.

Este estudo teve como objetivo analisar os sistemas de segurança da informação existentes, incluindo o NIST, a ISO 27001, os CIS Controls v8 e o framework do PPSI, para entender como as diretrizes desses modelos poderiam ser utilizados para fortalecer o PPSI, com um foco especial na segurança física. A metodologia adotada consistiu em uma análise documental dos modelos de segurança da informação e em uma comparação detalhada entre eles para identificar medidas que estivessem ausentes no framework do PPSI, mas que poderiam contribuir para o fortalecimento da segurança física. A partir dessa análise, foi possível elaborar uma lista de medidas de segurança que não estavam previstas no PPSI, organizadas de acordo com as categorias do ISO 27002. Essas medidas foram discutidas em termos de sua relevância para melhorar a proteção das instalações e ativos da administração pública federal.

O PPSI abrange o campo da segurança da informação cibernética, apresentando limitações no que se refere à segurança física dos ativos de informação. A proteção das instalações, equipamentos e documentos físicos, bem como a restrição de acesso a áreas sensíveis, são aspectos essenciais para a segurança da informação, mas não são tratados com a mesma profundidade no PPSI.

Os resultados mostraram que há diversas medidas importantes, especialmente no campo da segurança física, que poderiam ser incorporadas ao PPSI para fornecer uma proteção mais robusta e abrangente. Entre as medidas identificadas, destacam-se as relacionadas ao controle de acesso físico, monitoramento de instalações, proteção contra ameaças ambientais e a segurança durante o trabalho em áreas sensíveis. A adoção dessas medidas ajudaria a garantir que os ativos físicos e digitais da administração pública estejam adequadamente protegidos contra riscos diversos.

Assim, o estudo não apenas contribui para o fortalecimento da segurança da informação no setor público, mas também sugere uma integração eficaz de controles físicos, promovendo a construção de um modelo mais robusto e seguro.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002:2022 - Tecnologia da informação**: técnicas de segurança - Códigos de prática para gestão de segurança da informação. Rio de Janeiro, 2022.

AMINE, A. M.; CHAKIR, E. M.; ISSAM, T.; KHAMLICHI, Y. I. **A review of cybersecurity management standards applied in higher education institutions**. International Journal of Safety and Security Engineering, v. 13, n. 6, p. 1109-1116, 2023. Disponível em: https://doi.org/10.18280/ijsse.130614. Acesso em: 10 fev. 2025.

CENTER FOR INTERNET SECURITY. **CIS Controls v8**. 2023. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em: 11 fev. 2025.

CENTER FOR INTERNET SECURITY. **CIS Controls v8 Mapping to ISO/IEC 27002: 2022**. 2023. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-iso-iec2-27002-2022. Acesso em: 11 fev.
2025.

BOECHAR, Gabriela. **Sistema do governo é restabelecido após 6 dias de suposto ataque hacker**. Disponível em: https://www.cnnbrasil.com.br/politica/sistema-do-governo-e-restabelecido-apos-6-dias-de-suposto-ataque-hacker/. Acesso em 11 fev.
2025

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. **Institui a Política Nacional de Segurança da Informação**. Diário Oficial da União: seção 1, Brasília, DF, 27 dez. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.html. Acesso em: 11 fev. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852, de 28 de março de 2023. **Dispõe sobre o Framework de Privacidade e Segurança da Informação (PPSI) para a Administração Pública Federal**. Diário Oficial da União: seção 1, Brasília, DF, 29 mar. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 11 fev.
2025.

BRASIL. Secretaria de Governo Digital. **Guia do Framework de Privacidade e Segurança da Informação (PPSI)**. 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia$_framework_psi.pdf.Acessoem$: 11$fev.$2025.

BRASIL. Supremo Tribunal Federal. **Curso: Introdução à Proteção de Dados Pessoais**.

Disponível em: https://ead.stf.jus.br/course/view.php?id=508. Acesso em: 11 fev. 2025.

BPB ONLINE. **Yahoo data breach:** what actually happened. 2023. Disponível em: https://bpbonline.medium.com/yahoo-data-breach-what-actually-happened-54cf8f3f7c93. Acesso em: 11 fev. 2025.

FERNANDES, Oerton. **O impacto global da engenharia social e a importância das camadas de proteção**. 2023. Disponível em: https://www.linkedin.com/pulse/o-impacto-global-da-engenharia-social-e-import%C3%A2ncia-das-msc-com-or/?originalSubdomain=pt. Acesso em: 11 fev. 2025.

GAVIÃO, Luiz Octávio; SANTOS, Clarice Saraiva Andrade dos; OLIVEIRA, Leonardo Augusto dos Santos; PEREIRA, José Cristiano. **Proposta de avaliação da Política Nacional de Segurança da Informação por Processo de Análise Hierárquica**. Revista Perspectivas em Ciência da Informação, Belo Horizonte, v. 27, n. 4, p. 108-145, 2025. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/29373/32175. Acesso em: 10 fev. 2025.

GOULART, Eduardo; MADUREIRA, Vinicius. **Grupo hacker reivindicou autoria de ataque ao governo federal**. Disponível em: https://piaui.folha.uol.com.br/grupo-hacker-reivindicou-ataque-ao-governo-federal/. Acesso em 12 fev. 2025

GOUVEIA, Luís Borges. Gestão da segurança da informação. 2017. Instrução Normativa GSI Nº 1 - 27 de maio de 2020. **Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal**. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1%20de-27-de-maio-de-2020-258915215. Acesso em: 12 fev.
2025.

INTERNATIONAL Monetary Fund. 2024. **Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks**. Disponível em: https://www.imf.org/es/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024. Acesso em 10 fev. 2025

INSTRUÇÃO Normativa GSI Nº 2 - 24 de julho de 2020. **Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal**. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-2%20de-24-de-julho-de-2020-268684700. Acesso em: 12 fev. 2025.

INSTRUÇÃO Normativa GSI Nº 2 - 5 de fevereiro de 2013. **Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo,**

no âmbito do Poder Executivo Federal. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/IN02-GSI-PR-.pdf. Acesso em: 12 fev. 2025.

INSTRUÇÃO Normativa GSI Nº 3 - 28 de maio de 2021 **Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal**. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa%20gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 12 fev. 2025.

INSTRUÇÃO Normativa GSI Nº 3 - 6 de março de 2013 **Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal**. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1pagina=2data=14/03/2013. Acesso em: 12 fev. 2025.

INSTRUÇÃO Normativa GSI Nº 4 - 26 de março de 2020 **Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G**. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4%20de-26-de-marco-de-2020-250059468. Acesso em: 12 fev. 2025.

INSTRUÇÃO Normativa GSI Nº 5 - 31 de agosto de 2021 **Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal**. Disponível em: https://in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30%20de-agosto-de-2021-341649684. Acesso em: 12 fev. 2025.

INSTRUÇÃO Normativa GSI Nº 6 - 23 de dezembro de 2021 **Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal**. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-6-de-23-de-dezembro-de-2021-370081. Acesso em: 12 fev. 2025.

JOURDAIN, David. **Psicologia do hacker: como lidar com o invasor**. 2023. Disponível em: https://pt.linkedin.com/pulse/psicologia-do-hacker-como-lidar-com-o-invasor-david-jourdain-c7i5f. Acesso em: 11 fev. 2025.

QUERIDO, Guilherme Gondim. **Manual de boas práticas de segurança da informação para**

os sistemas de telemedicina tendo como base a norma ABNT NBR ISO/IEC 27002 e o framework CIS Controls. 2023. 128 f. Dissertação (Mestrado Profissional em Telemedicina e Telessaúde) – Faculdade de Ciências Médicas, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023. Disponível em: http://www.bdtd.uerj.br/handle/1/22780. Acesso em: 11 fev. 2025.

.