Resiliência cibernética em órgãos do SISP: diagnóstico do uso de controles selecionados do PPSI

Autor: Chesllen da Silva Pereira / **Orientador:** Prof. Dr. Luiz Antônio Ribeiro Júnior.

Resumo

Não é apenas o avanço da transformação digital iniciada nos anos 2000 que impõe novos desafios: a modernização das ameaças e a intensificação dos incidentes cibernéticos têm exigido que os órgãos da Administração Pública Federal superem um modelo de segurança restrito ao mínimo necessário em termos de controles, criando condições reais para o desenvolvimento de capacidades de resiliência cibernética. Nesse contexto, este artigo apresenta um diagnóstico da resiliência cibernética em uma amostra de 16 respondentes vinculados a órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), universo composto por mais de 250 órgãos federais, utilizando o Programa de Privacidade e Segurança da Informação (PPSI) como referência. Para isso, foi aplicado um questionário estruturado, desenvolvido no Microsoft Forms com base em controles selecionados do PPSI, cujas respostas foram analisadas por meio de uma abordagem quantitativa e qualitativa, combinando estatística descritiva para as questões fechadas e análise de conteúdo para as respostas abertas. Os resultados apontam a existência de uma base relevante de controles implementados: aproximadamente 90% dos respondentes relataram rotinas formais de cópia de segurança de dados essenciais, cerca de 80% indicaram segmentação de rede e quase 90% declararam uso de mecanismos de prevenção de intrusão. Contudo, observam-se lacunas importantes em aspectos como a desativação da execução automática de mídias removíveis e o bloqueio de portas USB (presentes em apenas metade da amostra), o uso mais avançado de filtragem em camada de aplicação, a centralização da gestão antimalware e a baixa frequência de testes formais de recuperação e resposta a incidentes, realizados de forma estruturada por menos da metade dos órgãos. A autoavaliação de maturidade concentra-se nos níveis “Definido” e “Gerenciado”, com minoria se percebendo em estágio “Otimizado”, e confiança predominantemente média ou alta na capacidade de recuperação, ainda que apoiada em processos pouco testados na prática. As principais dificuldades relatadas envolvem escassez de recursos humanos e financeiros, desafios de conscientização e engajamento da alta gestão e dependência de sistemas legados complexos. O estudo contribui ao oferecer um panorama integrado da resiliência cibernética nesses órgãos e das dificuldades cotidianas para consolidar capacidades de prevenção, resposta e recuperação em caso de desastres ou ataques cibernéticos, além de apontar caminhos para o aperfeiçoamento do instrumento de diagnóstico e para ciclos futuros de avaliação da resiliência cibernética no âmbito do SISP.

Palavras-chave: Resiliência cibernética; Segurança da informação; Administração pública; SISP; PPSI.

1 Introdução

A crescente digitalização dos serviços públicos e a intensificação da dependência de Tecnologias da Informação e Comunicação (TIC) na Administração

Pública Federal ampliam significativamente a superfície de exposição a incidentes cibernéticos. Ataques de ransomware, vazamentos de dados, indisponibilidade prolongada de sistemas críticos e fraudes digitais passaram a compor o cotidiano dos órgãos governamentais, o que exige não apenas a adoção de controles de segurança pontuais, mas a construção de uma capacidade contínua de prevenir, resistir, responder e se recuperar de eventos adversos, em linha com a Estratégia Nacional de Cibersegurança - E-Ciber, que coloca a segurança e a resiliência dos serviços essenciais e das infraestruturas críticas como eixos centrais da política nacional de cibersegurança (CASA CIVIL, 2025).

Desde o início dos anos 2000, essa trajetória tem sido marcada por iniciativas sucessivas de governo eletrônico e governo digital, estruturadas em programas e políticas que buscam ampliar o uso de TIC na prestação de serviços públicos, conforme sintetizado na linha do tempo oficial “Do Eletrônico ao Digital”, que apresenta a evolução dessas ações no âmbito federal (SGD/MGI, 2019).

No âmbito do Governo Federal, o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) organiza e coordena os órgãos da administração direta, autárquica e fundacional em torno de diretrizes comuns de governança digital, segurança da informação e gestão de TIC, tendo sido instituído pelo Decreto nº 7.579, de 11 de outubro de 2011 (CASA CIVIL, 2011). Entre os instrumentos estruturantes dessa agenda, destaca-se o Programa de Privacidade e Segurança da Informação (PPSI), estabelecido pela Portaria SGD/MGI nº 852, de 28 de março de 2023, com o objetivo de elevar a maturidade e a resiliência, em termos de privacidade e segurança da informação, no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional que compõem o SISP (SGD/MGI, 2023). O PPSI caracteriza-se como um conjunto de projetos e processos distribuídos nas áreas temáticas de governança, maturidade, metodologia, pessoas e tecnologia, e institui o Framework de Privacidade e Segurança da Informação, composto por controles, metodologias e ferramentas de apoio, que funcionam como referencial mínimo para que os órgãos integrantes do SISP planejem, implementem e monitorem suas práticas de segurança e privacidade de forma alinhada aos marcos legais e estratégicos nacionais.

Apesar da existência de diretrizes e frameworks institucionais de governança digital, a realidade dos órgãos públicos é marcada por forte heterogeneidade em

termos de porte, complexidade de sistemas, disponibilidade de recursos humanos e orçamentários, maturidade em governança de TI e nível de priorização da temática pela alta gestão. Conforme discutem Rodrigues e Cammarosano (2022), a consolidação da governança digital no Brasil ainda enfrenta desafios para garantir a efetividade das ações e do processo administrativo eletrônico, o que envolve capacidade estatal, coordenação entre órgãos e integração da agenda digital às estratégias institucionais. Esse cenário afeta diretamente a capacidade de estruturar e sustentar iniciativas consistentes de segurança da informação e privacidade. A própria Portaria SGD/MGI nº 852/2023 reconhece a necessidade de diagnósticos periódicos, autoavaliações e planos de trabalho para implementação gradual do framework, indicando que ainda há um caminho relevante a percorrer para que os controles de privacidade e segurança da informação sejam plenamente incorporados pela Administração Pública Federal (SGD/MGI, 2023).

Diante desse contexto, torna-se fundamental dispor de diagnósticos que permitam compreender, de forma estruturada, como os órgãos estão operacionalizando as diretrizes de segurança e privacidade, quais controles estão efetivamente implementados e quais são as percepções e dificuldades no caminho para uma maior resiliência cibernética. A pesquisa desenvolvida neste trabalho toma como base uma amostra de órgãos integrantes do SISP e, a partir da perspectiva de profissionais que atuam diretamente na gestão de TIC, segurança da informação e privacidade, busca levantar informações sobre políticas, processos, infraestrutura, continuidade, governança e percepção de maturidade, utilizando o framework do PPSI, instituído pela Portaria SGD/MGI nº 852/2023, como referência para a estruturação do instrumento de coleta. Dessa forma, a amostra analisada funciona como um recorte de realidades institucionais diversas, permitindo identificar convergências, diferenças e pontos críticos que tendem a se repetir em diferentes contextos da Administração Pública Federal.

Nesse sentido, o presente artigo tem por objetivo realizar um diagnóstico da resiliência cibernética em uma amostra de órgãos integrantes do SISP, utilizando os controles do PPSI como base de referência. Especificamente, busca-se analisar o grau de aderência dos órgãos da amostra aos controles fundamentais do PPSI, identificando avanços, lacunas e diferenças na implementação de políticas, processos e controles técnicos, bem como avaliar, com base nos dados da pesquisa, a

maturidade das práticas de resiliência cibernética relacionadas à cultura organizacional, gestão de riscos, continuidade, resposta a incidentes e monitoramento, em alinhamento às diretrizes estabelecidas para o programa (SGD/MGI, 2023).

Além desta introdução, o artigo está organizado em quatro seções principais. A Seção 2 apresenta o referencial teórico, discutindo resiliência cibernética, frameworks internacionais e o contexto da Administração Pública Federal. A Seção 3 descreve a metodologia adotada, detalhando a escolha dos controles, o instrumento de pesquisa, a amostra e os procedimentos de análise. A Seção 4 traz os resultados e discussões, organizados em blocos temáticos de controles tecnológicos, fator humano, processos, software livre e maturidade. Por fim, as Seções 5 e 6 apresentam, respectivamente, as principais conclusões do estudo e os próximos passos de pesquisa, seguidas dos anexos com o instrumento utilizado.

2 REFERENCIAL TEÓRICO

2.1 Resiliência cibernética e fator humano

Neste artigo, adota-se uma compreensão de resiliência cibernética alinhada ao NIST Cybersecurity Framework (CSF) 2.0, que trata a gestão de riscos de cibersegurança como um processo contínuo e integrado às funções de Governar, Identificar, Proteger, Detectar, Responder e Recuperar, voltado a manter e restaurar funções essenciais da organização diante de incidentes (NIST, 2024). Essa perspectiva parte do reconhecimento de que violações, interrupções e falhas fazem parte do ambiente digital moderno e de que a gestão de riscos deve contemplar não apenas a proteção preventiva, mas também a capacidade de se preparar, absorver impactos, recuperar e adaptar, de forma contínua, processos, tecnologias e estruturas organizacionais.

O Data Breach Investigations Report (DBIR) 2024 indica que o “elemento humano” esteve presente em 68% das violações analisadas, considerando erros, credenciais comprometidas e sucesso de campanhas de engenharia social, o que evidencia a centralidade do comportamento e das decisões dos usuários na superfície de exposição das organizações (VERIZON, 2024). Esses dados reforçam que programas sistemáticos de conscientização, treinamento e fortalecimento da cultura

de segurança são componentes estruturais da resiliência, ao lado de controles técnicos e de processos maduros de resposta a incidentes.

Relatórios globais sobre o custo de incidentes também evidenciam o impacto estrutural das falhas de segurança. O Cost of a Data Breach Report 2024, da IBM Security, aponta custo médio global de 4,88 milhões de dólares por violação, o maior aumento percentual desde a pandemia, e destaca o phishing como um dos vetores de ataque mais frequentes e onerosos (IBM SECURITY, 2024).

O relatório mostra ainda que organizações que empregam extensivamente automação e inteligência artificial em segurança reduzem de forma significativa o tempo de identificação e contenção de incidentes, bem como o custo médio por violação, enquanto arquiteturas pouco governadas e controles de acesso frágeis em sistemas de IA tendem a ampliar o impacto financeiro.

Esses achados reforçam que a resiliência depende da combinação entre tecnologia, preparo organizacional e competências humanas, por meio de processos maduros de resposta a incidentes, monitoramento contínuo e gestão estruturada de identidades e acessos (IBM SECURITY, 2024).

2.2 Segurança da informação e resiliência na Administração Pública Federal

No setor público, a abordagem resiliente assume relevância particular, uma vez que incidentes cibernéticos afetam diretamente a continuidade de políticas públicas, a prestação de serviços e a proteção de dados pessoais de cidadãos. No Brasil, o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) reúne órgãos da administração direta, autárquica e fundacional com responsabilidades específicas na gestão e na governança de tecnologia e segurança. Auditoria operacional recente do Tribunal de Contas da União em organizações do SISP constatou que essas entidades se encontram aquém do esperado na implementação de medidas de cibersegurança, sem evidências de que alguma atinja integralmente o grupo de implementação básico (IG1) dos CIS Controls, o que indica exposição relevante a ataques cibernéticos e baixa maturidade de segurança da informação em parte expressiva da Administração Pública Federal (TCU, 2024).

Para enfrentar esse cenário, a Secretaria de Governo Digital instituiu o Programa de Privacidade e Segurança da Informação (PPSI), por meio da Portaria SGD/MGI nº 852/2023, estabelecendo um framework de controles estruturados e adaptados à realidade da Administração Pública Federal (SGD/MGI, 2023). O PPSI organiza um conjunto de medidas distribuídas em temas como governança, maturidade, pessoas e tecnologia, com o objetivo de apoiar os órgãos do SISP na elevação de sua capacidade de privacidade e segurança da informação, por meio de diagnósticos, planos de trabalho e instrumentos de apoio à implementação de controles.

2.3 Frameworks normativos e o PPSI

No plano internacional, o NIST Cybersecurity Framework consolidou-se como referência de alto nível para a gestão de riscos de segurança, ao organizar suas diretrizes nas funções Governar, Identificar, Proteger, Detectar, Responder e Recuperar, enfatizando a integração entre governança corporativa e práticas de cibersegurança (NIST, 2024). Essa estrutura fornece um vocabulário comum e um conjunto de resultados esperados que podem ser adaptados a diferentes setores e níveis de maturidade, servindo como base para a definição de políticas, processos e métricas de segurança.

De forma complementar, a norma ISO/IEC 27001:2022 estabelece requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), abrangendo políticas, processos, responsabilidades, gestão de riscos e controles de segurança em um ciclo de melhoria contínua, sendo amplamente utilizada como referência por organizações públicas e privadas em todo o mundo (ISO; IEC, 2022). Em sua versão atualizada, os controles associados são detalhados na ISO/IEC 27002:2022 e organizados em quatro grupos – organizacionais, de pessoas, físicos e tecnológicos –, oferecendo um catálogo estruturado de medidas que podem ser selecionadas conforme o contexto e o apetite de risco da organização.

No contexto brasileiro, esses referenciais dialogam com marcos nacionais como a Estratégia Nacional de Cibersegurança – E-Ciber, a Lei Geral de Proteção de Dados (LGPD) e os normativos específicos para a Administração Pública Federal, que enfatizam a necessidade de gestão sistemática de riscos, proteção de dados pessoais e continuidade de serviços essenciais. O Programa de Privacidade e Segurança da

Informação (PPSI), instituído pela Portaria SGD/MGI nº 852/2023, materializa essa convergência ao propor um framework próprio para os órgãos integrantes do SISP, inspirado em boas práticas internacionais (como o NIST CSF, os CIS Controls e as normas ISO/IEC 27000) e adaptado às particularidades da gestão pública federal (SGD/MGI, 2023; PPSI, 2025). Assim, o PPSI funciona como um referencial normativo que traduz esses frameworks em diretrizes, processos e instrumentos de apoio à elevação da maturidade em privacidade e segurança da informação no âmbito do SISP.

3 Metodologia

3.1 Tipo de pesquisa e abordagem

A pesquisa é de natureza aplicada, com objetivos exploratório-descritivos, pois visa produzir conhecimento voltado à solução de problemas concretos da Administração Pública Federal e, ao mesmo tempo, descrever e interpretar o fenômeno estudado (GIL, 2019).

Adotou-se abordagem quali-quantitativa, combinando técnicas quantitativas úteis, para descrever a distribuição de respostas e o grau de implementação de controles, e qualitativas, adequadas para captar percepções, significados e desafios relatados pelos participantes (MINAYO, 2025).

3.2 População, amostra e critérios de seleção

A população (ou universo) de interesse deste estudo corresponde aos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal, ou seja, mais de 250 órgãos federais para os quais o Programa de Privacidade e Segurança da Informação (PPSI) foi concebido (MGI, 2025). Considerando restrições de tempo e acesso, optou-se por uma amostragem não probabilística por conveniência. O questionário foi divulgado, por meio de correio eletrônico institucional e redes de contato profissional, a servidores que atuam em unidades de TIC, segurança da informação ou privacidade em órgãos do SISP, convidando-os a participar voluntariamente da pesquisa.

A amostra final é composta por 16 respondentes vinculados a diferentes órgãos do SISP, o que representa uma fração pequena do universo de mais de 250 órgãos

integrantes do sistema, mas contempla realidades distintas em termos de estrutura, recursos, maturidade e perfil organizacional. Para preservar o anonimato, o instrumento não coleta o nome do órgão nem do respondente. Em função do tamanho reduzido da amostra e da estratégia de seleção adotada, optou-se por analisar os resultados de forma agregada, sem estratificação por tipo de órgão ou porte. Esse recorte não permite generalizações estatísticas para todo o SISP, mas oferece um panorama inicial útil para compreender tendências e desafios recorrentes.

3.3 Instrumento de coleta e seleção dos controles do PPSI

O instrumento de coleta de dados foi um questionário estruturado, elaborado pelo autor com base no Framework de Privacidade e Segurança da Informação do PPSI (SGD/MGI, 2023; PPSI, 2025) e implementado na plataforma Microsoft Forms. Inicialmente, foram analisados os guias e documentos de apoio do programa, buscando identificar quais controles apresentavam relação mais direta com a resiliência operacional das instituições – isto é, com a capacidade de prevenir, resistir, responder e recuperar-se de incidentes de segurança.

A partir dessa leitura, foram selecionados os controles 10 (Defesas contra malware), 11 (Recuperação de dados), 13 (Monitoramento e defesa da rede), 14 (Conscientização e treinamento em segurança), 17 (Gestão de resposta a incidentes), 22 (Políticas e processos de privacidade) e 23 (Conscientização e treinamento em privacidade). Para cada um deles, o questionário inclui itens que avaliam o nível de implementação das principais medidas previstas, utilizando a escala recomendada pelos materiais do PPSI: “Totalmente implementado”, “Parcialmente implementado”, “Não implementado” e “Não se aplica”.

Além desses itens diretamente associados aos controles, o instrumento incorpora questões de percepção sobre suficiência do ferramental tecnológico, comportamento dos colaboradores enquanto “firewall humano”, efetividade dos treinamentos, clareza e eficácia dos processos, nível de maturidade em resiliência cibernética, confiança na capacidade de recuperação diante de incidentes graves, frequência de testes práticos (como exercícios de recuperação de desastres ou simulações de ataque), principais desafios para evolução da resiliência e diretriz

institucional quanto ao uso de software livre. O questionário completo é apresentado no Anexo A, com a numeração das questões que subsidiam cada bloco de análise.

3.4 Procedimentos de coleta, tratamento e análise dos dados

A coleta de dados foi realizada em 2025, por meio do envio do link do formulário aos participantes. As respostas foram exportadas da plataforma e organizadas em planilhas eletrônicas para tratamento. Na dimensão quantitativa, aplicou-se estatística descritiva (frequências absolutas e relativas, distribuições percentuais e sínteses em tabelas e gráficos) para cada item dos controles e das questões de percepção. Nas questões em que a resposta era opcional e houve menos de 16 respondentes, os percentuais foram calculados apenas sobre as respostas válidas, de forma a evitar distorções.

Para a dimensão qualitativa, em especial as questões abertas sobre justificativas, principais desafios e softwares livres utilizados, empregou-se análise de conteúdo temática, segundo os procedimentos propostos por Bardin (2016). As respostas foram lidas de forma exaustiva, codificadas e agrupadas em categorias, permitindo identificar padrões, recorrências e relações entre domínios. Foi a partir desse processo que se consolidaram, por exemplo, os três eixos centrais de desafios discutidos na Seção 4.5.2.

Ao longo da discussão dos resultados, os achados empíricos foram confrontados, de forma seletiva, com a literatura e documentos de referência apresentados na Seção 2 – como o DBIR (VERIZON, 2024), o Cost of a Data Breach Report (IBM SECURITY, 2024), a auditoria do TCU (2024) e os referenciais normativos de segurança e privacidade –, buscando evidenciar convergências, divergências e implicações para a resiliência cibernética dos órgãos analisados.

4 Resultados e Discussões

Nesta seção são analisados, em blocos temáticos, os principais grupos de controles avaliados na pesquisa: (I) controles tecnológicos (Controles 10, 11 e 13, além da percepção sobre suficiência de ferramentas); (II) fator humano, conscientização e treinamentos (Controles 14 e 23 e percepção sobre o “firewall humano”); (III) processos de privacidade, gestão de incidentes e continuidade

(Controles 17 e 22 e avaliação de eficácia e testes); (IV) diretrizes e ecossistema de software livre; e (V) maturidade percebida e desafios. As evidências foram obtidas a partir das respostas dos órgãos integrantes do SISP que compõem a amostra pesquisada. As análises do Bloco 4.1 tomam como referência as respostas às questões 1 a 7 do questionário (ver Anexo A).

4.1 Bloco Controles 10, 11 e 13 e percepção sobre ferramentas

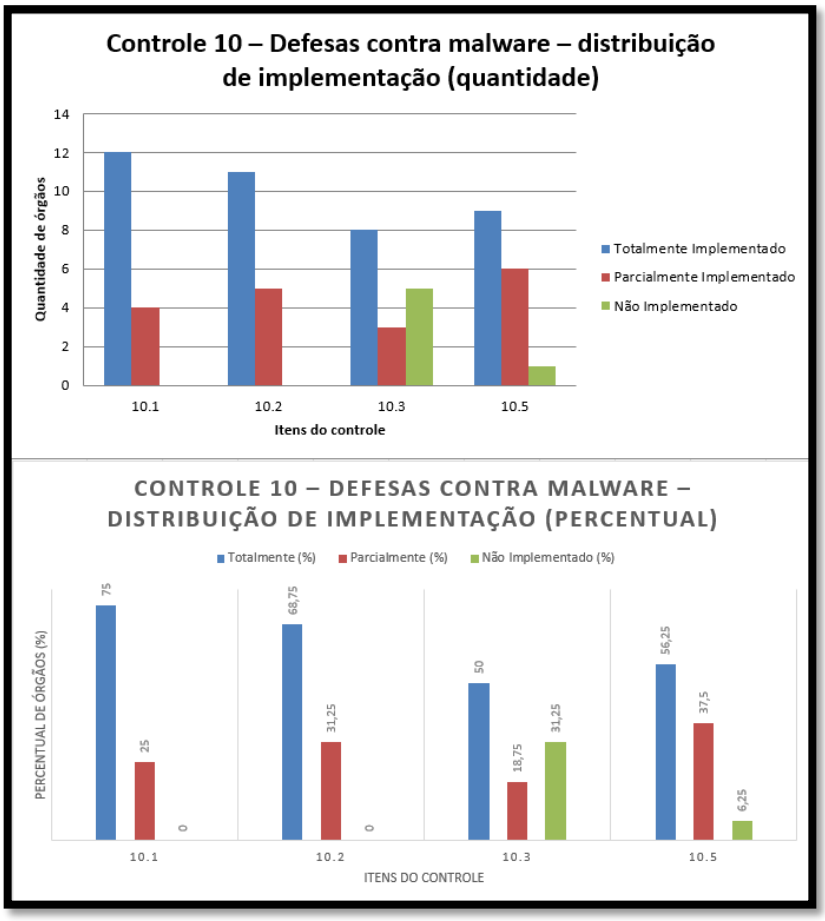
4.1.1 Controle 10 – Defesas contra malware

No que se refere ao Controle 10 (defesas contra malware), observa-se um nível relativamente elevado de implementação formal. Em relação ao requisito de implementar e manter defesas contra malware nos ativos da organização, 75,0% dos órgãos participantes (12 de 16) indicaram ter o controle totalmente implementado, enquanto 25,0% (4 de 16) o classificaram como parcialmente implementado. Resultado semelhante aparece quanto à configuração de atualizações automáticas de assinaturas antimalware, com 68,8% dos órgãos (11 de 16) relatando implementação total e 31,2% (5 de 16) implementação parcial.

Por outro lado, alguns aspectos específicos apresentam lacunas relevantes. A desativação da execução automática de mídias removíveis, medida tradicionalmente considerada crítica para mitigar a introdução de código malicioso por dispositivos externos, encontra-se totalmente implementada em apenas 50,0% dos órgãos (8 de 16). Em 18,8% dos casos (3 de 16) o controle é apenas parcialmente implementado e, em 31,2% (5 de 16), não há implementação. Esses resultados indicam que, embora a maior parte dos órgãos mantenha soluções antimalware em operação, ainda existem brechas importantes em vetores clássicos de ataque.

A gestão centralizada das soluções antimalware também revela um cenário misto. Pouco mais da metade dos órgãos analisados (56,2%, 9 de 16) declara gestão totalmente centralizada, enquanto 37,5% (6 de 16) possui apenas gestão parcial e 6,2% (1 de 16) não possui centralização. Isso sugere que, em parcela não desprezível dos ambientes analisados, ainda podem existir “ilhas” de proteção geridas de forma descentralizada, o que dificulta a correlação de eventos, a atualização homogênea de assinaturas e a aplicação consistente de políticas de segurança.

Figura 1 – Controle 10 – Defesas contra malware – distribuição de implementação.



Fonte: Elaborado pelo autor (2025)

4.1.2 Controle 11 – Backup e recuperação de dados

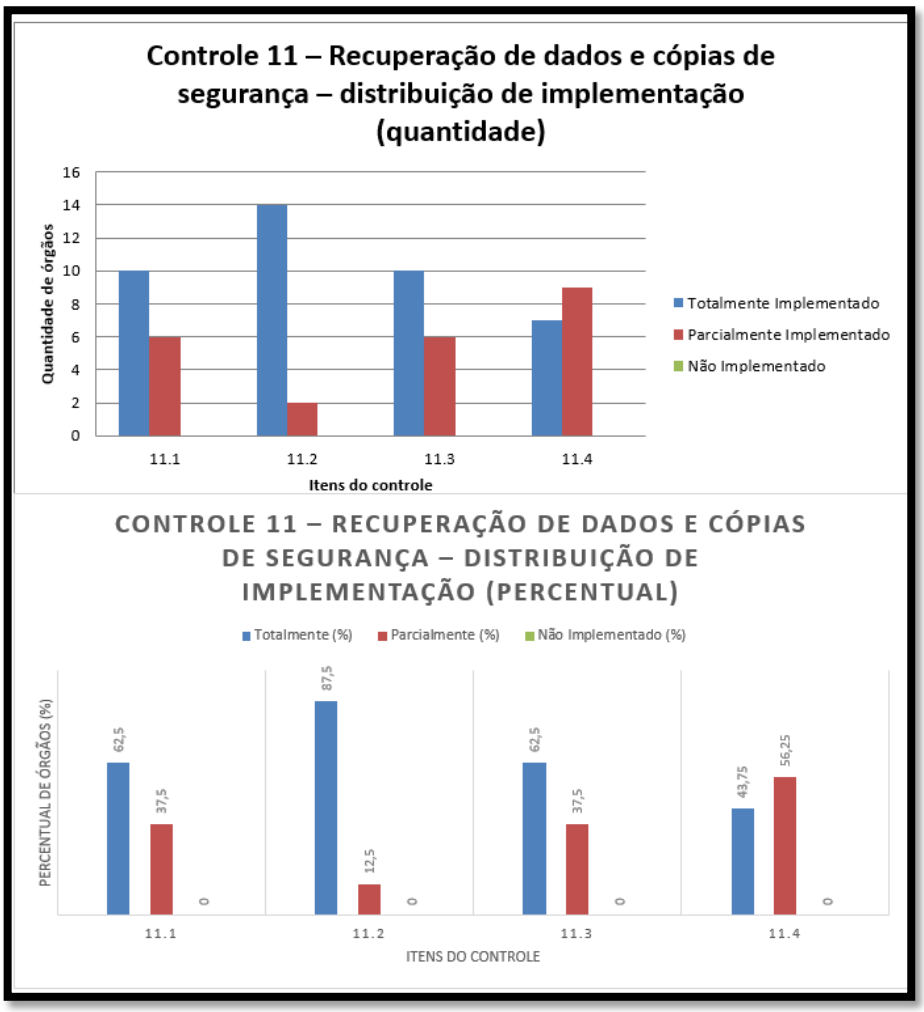
Os resultados relativos ao Controle 11 (recuperação de dados e cópias de segurança) indicam uma adesão mais robusta em comparação com outros grupos de controles. O estabelecimento de um processo formal de recuperação de dados é declarado como totalmente implementado por 62,5% dos órgãos (10 de 16), ao passo que 37,5% (6 de 16) relatam implementação parcial. A realização de cópias de segurança das informações necessárias à continuidade dos serviços essenciais apresenta o melhor desempenho do bloco: 87,5% dos órgãos (14 de 16) afirmam ter o controle totalmente implementado, e apenas 12,5% (2 de 16) o classificam como parcialmente implementado.

A proteção dos dados de backup contra acesso não autorizado, modificação ou destruição mantém patamar semelhante ao do processo de recuperação: 62,5% dos

órgãos (10 de 16) indicam implementação total e 37,5% (6 de 16) implementação parcial. No entanto, quando se analisa a prática de testar periodicamente a capacidade de recuperação dos dados de backup, observa-se um recuo sensível: apenas 43,8% dos órgãos (7 de 16) realizam testes de forma plenamente estruturada, enquanto 56,2% (9 de 16) o fazem apenas parcialmente.

Esse descompasso sugere que, embora as rotinas de backup estejam amplamente difundidas, a validação efetiva da recuperabilidade ainda não é um processo maduro na maioria dos órgãos. Em termos de resiliência cibernética, isso implica que uma parte significativa das organizações pode descobrir falhas em seus procedimentos de recuperação apenas em situações reais de incidente, aumentando o risco de indisponibilidade prolongada e perda de dados críticos.

Figura 2 – Controle 11 – Recuperação de dados e cópias de segurança – distribuição de implementação



Fonte: Elaborado pelo autor (2025)

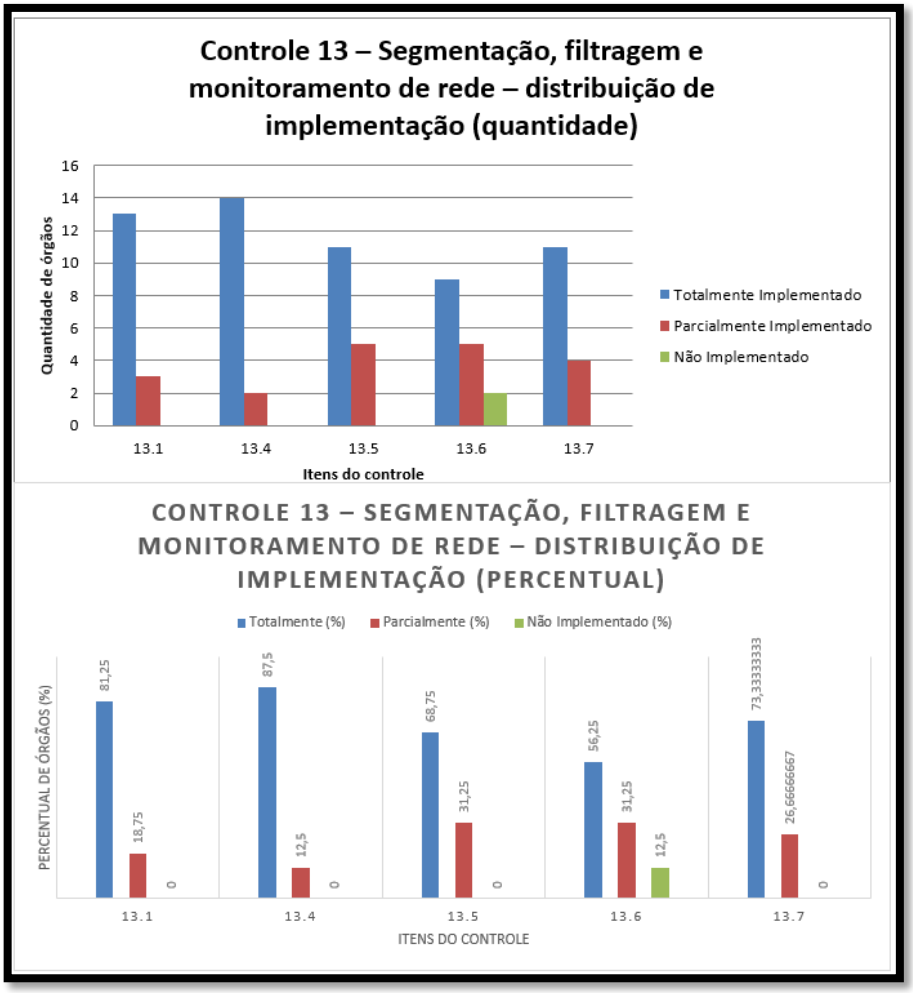
4.1.3 Controle 13 – Segmentação, filtragem e monitoramento de rede

Os controles ligados à proteção e monitoramento de rede (Controle 13) apresentam, em geral, bons níveis de adoção, embora ainda existam lacunas em funcionalidades mais avançadas. A filtragem de tráfego entre segmentos de rede está totalmente implementada em 81,2% dos órgãos (13 de 16), com 18,8% (3 de 16) indicando implementação parcial. As soluções de prevenção de intrusão de rede aparecem como um dos pontos mais positivos: 87,5% dos órgãos (14 de 16) reportam implementação total e 12,5% (2 de 16) parcial.

O controle de acesso a nível de porta, importante para restringir dispositivos não autorizados na rede, é totalmente implementado por 68,8% dos órgãos (11 de 16), enquanto 31,2% (5 de 16) indicam adoção parcial. Já a filtragem em camada de aplicação, associada a capacidades mais sofisticadas de inspeção de tráfego, apresenta um cenário um pouco menos maduro: 56,2% dos órgãos (9 de 16) afirmam ter o controle totalmente implementado, 31,2% (5 de 16) relatam implementação parcial e 12,5% (2 de 16) não possuem tal capacidade.

A centralização de alertas de eventos de segurança, típica de soluções de correlação e monitoramento, está totalmente implementada em 73,3% dos órgãos que responderam à questão (11 de 15), com 26,7% (4 de 15) reportando implementação parcial. Esses resultados indicam que a maioria dos ambientes analisados dispõe de ao menos algum nível de monitoramento centralizado, mas ainda há margem para evolução na integração de fontes de log e na automação da detecção de incidentes.

Figura 3 – Controle 13 – Segmentação, filtragem e monitoramento de rede – distribuição de implementação



Fonte: Elaborado pelo autor (2025).

4.1.4 Percepção sobre a suficiência das ferramentas

A questão sobre a suficiência das ferramentas complementa a visão objetiva dos controles tecnológicos com a percepção dos participantes. A maioria dos órgãos (68,8%, 11 de 16) considera que possui um conjunto de ferramentas “suficientes”, isto é, adequadas para operar e garantir a proteção básica, ainda que reconheça possíveis lacunas de integração. Em 25,0% dos casos (4 de 16), o ferramental é classificado como “básico, com lacunas”, indicando presença de ferramentas mínimas, porém com faltas relevantes ou soluções obsoletas que exigem maior esforço manual. Apenas 6,2% das respostas (1 de 16) indicam um cenário em que as ferramentas excedem as necessidades, caracterizando um ambiente mais robusto e proativo.

De forma geral, a percepção de suficiência é coerente com os resultados objetivos: existe uma base razoável de proteção, especialmente em backup e

segmentação de rede, mas ainda há deficiências importantes em pontos específicos, como o bloqueio de execução automática de mídias removíveis, os testes periódicos de recuperação de backup e o uso mais avançado de filtragem em camada de aplicação. Esses elementos tendem a se tornar pontos de atenção prioritários para elevar a resiliência cibernética dos órgãos da amostra. Tal quadro é compatível com diagnósticos mais amplos sobre a Administração Pública Federal, nos quais se observa a presença de controles mínimos em grande parte das organizações, mas também lacunas relevantes em práticas de monitoramento, continuidade e validação periódica de capacidades críticas (TCU, 2024; ISO; IEC, 2022).

Tabela 1 – Implementação dos controles 10, 11 e 13 do PPSI na amostra em % de respostas.

Medida (Controle)	Totalmente impl	Parcialmente impl	Não impl	Não se aplica
10.1 – Defesas contra malware nos ativos da organização	75,0%	25,0%	0,0%	0,0%
10.2 – Atualizações automáticas de assinaturas antimalware	68,8%	31,2%	0,0%	0,0%
10.3 – Desativação da execução automática de mídias removíveis	50,0%	18,8%	31,2%	0,0%
10.5 – Gestão centralizada das soluções antimalware	56,2%	37,5%	6,2%	0,0%
11.1 – Processo formal de recuperação de dados	62,5%	37,5%	0,0%	0,0%
11.2 – Cópias de segurança das informações essenciais	87,5%	12,5%	0,0%	0,0%
11.3 – Proteção dos dados de backup contra acesso/modificação indevidos	62,5%	37,5%	0,0%	0,0%
11.4 – Testes periódicos de recuperação dos dados de backup	43,8%	56,2%	0,0%	0,0%
13.1 – Filtragem de tráfego entre segmentos de rede	81,2%	18,8%	0,0%	0,0%
13.4 – Soluções de prevenção de intrusão de rede	87,5%	12,5%	0,0%	0,0%
13.5 – Controle de acesso em nível de porta	68,8%	31,2%	0,0%	0,0%
13.6 – Filtragem em camada de aplicação	56,2%	31,2%	12,5%	0,0%

13.7 – Centralização de alertas de eventos de segurança*	73,3%	26,7%	0,0%	0,0%

Fonte: Elaborado pelo autor (2025)

4.2 Bloco Controles 14 e 23, comportamento de usuários e treinamentos

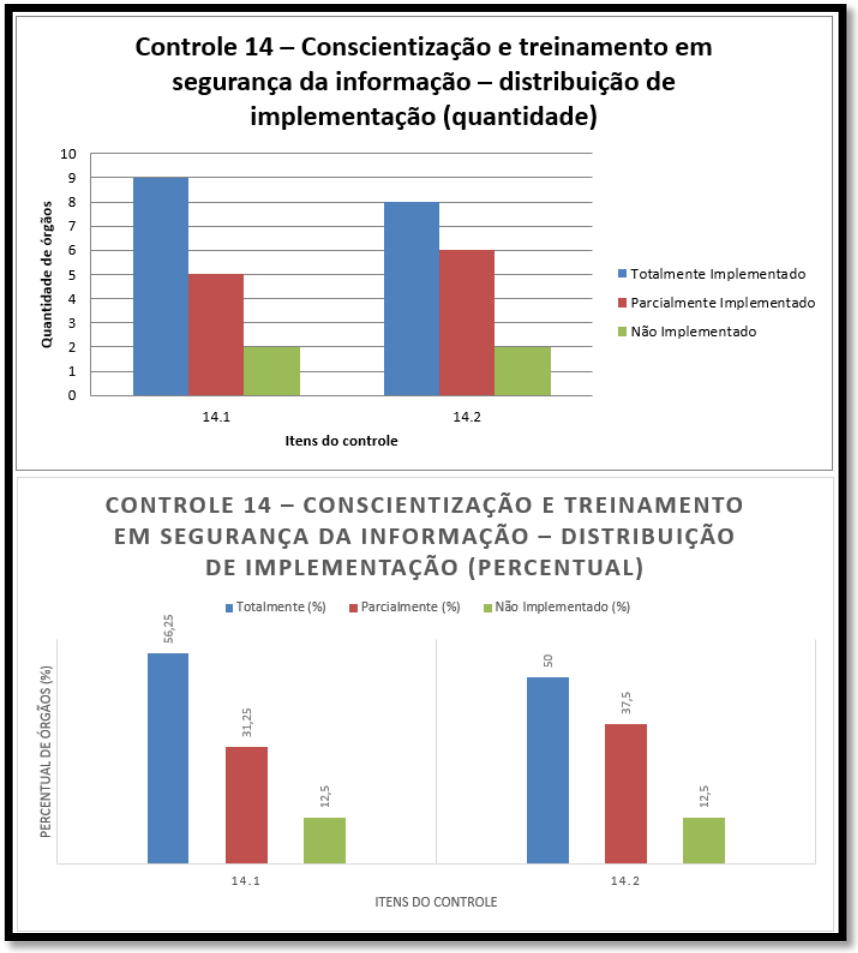
O Bloco 4.2 reúne os resultados relativos aos controles de conscientização e treinamento em segurança e privacidade, bem como à percepção sobre o comportamento dos usuários e a efetividade das ações de capacitação. As análises desta subseção baseiam-se principalmente nas respostas às questões 8 a 11 e 17 e 18 do questionário (ver Anexo A).

4.2.1 Controle 14 – Programas de conscientização em segurança da informação

O Controle 14 trata do estabelecimento de programas de conscientização em segurança da informação e do treinamento da força de trabalho sobre suas responsabilidades. Em relação à existência de um programa de conscientização estruturado, 56,2% dos órgãos (9 de 16) declaram implementação total, 31,2% (5 de 16) relatam implementação parcial e 12,5% (2 de 16) não possuem o controle implementado. Quanto ao treinamento sobre responsabilidades em segurança da informação, 50,0% dos órgãos (8 de 16) indicam implementação total, 37,5% (6 de 16) parcial e 12,5% (2 de 16) não implementado.

Esses resultados sugerem que a maioria dos órgãos da amostra já dispõe de iniciativas formais de sensibilização e capacitação em segurança, mas ainda existem casos em que os programas são inexistentes ou pouco estruturados, o que tende a impactar diretamente o comportamento dos usuários frente a riscos cibernéticos.

Figura 4: Controle 14 – Conscientização e treinamento em segurança da informação



Fonte: Elaboração própria (2025)

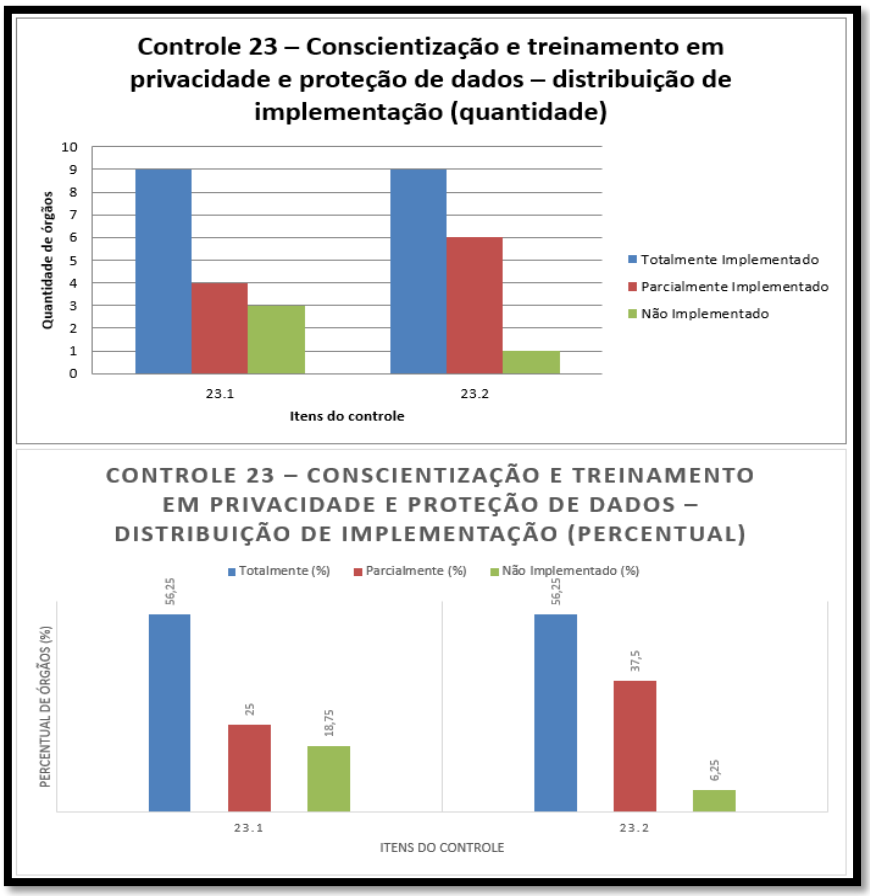
4.2.2 Controle 23 – Programas de conscientização em privacidade e proteção de dados

No que se refere ao Controle 23, voltado à conscientização em privacidade e proteção de dados, o cenário é semelhante, porém ligeiramente mais heterogêneo. A existência de um programa formal de conscientização em privacidade é relatada como totalmente implementada por 56,2% dos órgãos (9 de 16), enquanto 25,0% (4 de 16) indicam implementação parcial e 18,8% (3 de 16) não possuem tal programa. Em relação aos treinamentos específicos em privacidade e proteção de dados para a força de trabalho, 56,2% dos órgãos (9 de 16) declaram implementação total, 37,5% (6 de 16) parcial e apenas 6,2% (1 de 16) não implementado.

Observa-se, portanto, que a pauta de privacidade já se encontra incorporada à agenda de capacitação de grande parte dos órgãos analisados, ainda que uma fração

relevante não disponha de programas estruturados, o que pode dificultar a consolidação de uma cultura consistente de proteção de dados pessoais.

Figura 5: Controle 23 – Conscientização e treinamento em privacidade e proteção de dados



Fonte: Elaborado pelo autor (2025)

4.2.3 Percepção sobre o “firewall humano” e efetividade dos treinamentos

A percepção dos participantes sobre o fator humano confirma a importância desses programas. Quando convidados a classificar o comportamento dos usuários, 56,2% das respostas (9 de 16) descrevem o quadro como de “usuários conscientes”, que entendem riscos básicos e tentam seguir as políticas, mas não são plenamente proativos. Em 31,2% dos órgãos (5 de 16), o fator humano é descrito como “reativo”, ou seja, os usuários só se preocupam com segurança quando são cobrados ou após incidentes. Apenas 12,5% (2 de 16) enxergam seu corpo funcional como “aliado proativo”, vigilante e engajado na identificação ativa de ameaças.

Essa percepção é coerente com a avaliação da efetividade dos treinamentos. A ampla maioria dos órgãos (81,2%, 13 de 16) considera os treinamentos “moderadamente efetivos”, produzindo melhora temporária de atenção, mas com retorno relativamente rápido a antigos hábitos. Apenas 12,5% (2 de 16) avaliam os treinamentos como “muito efetivos”, com impacto claro e sustentado na cultura de segurança, enquanto 6,2% (1 de 16) indicam treinamentos inefetivos ou inexistentes.

Em síntese, os dados indicam que, embora a maior parte dos órgãos da amostra já possua programas de conscientização e treinamento em segurança e privacidade, esses programas ainda não resultam, na maior parte dos casos, em uma postura amplamente proativa por parte dos usuários. O fator humano permanece como componente crítico da resiliência cibernética, exigindo ações contínuas de educação, reforço de mensagens e envolvimento da alta gestão. Essa centralidade do elemento humano e a dificuldade em consolidar comportamentos proativos dialogam diretamente com os achados de relatórios internacionais, que apontam a participação de erros humanos, credenciais comprometidas e engenharia social em parcela significativa das violações (VERIZON, 2024; IBM SECURITY, 2024).

4.3 Bloco Controles 17 e 22, eficácia e testes de continuidade

O Bloco 4.3 aborda os processos formais de gestão de incidentes, políticas e procedimentos de privacidade e a forma como esses processos são percebidos em termos de eficácia, confiança na recuperação e validação prática. As evidências apresentadas nesta subseção derivam das respostas às questões 12 a 16, 20 e 21 do questionário (ver Anexo A).

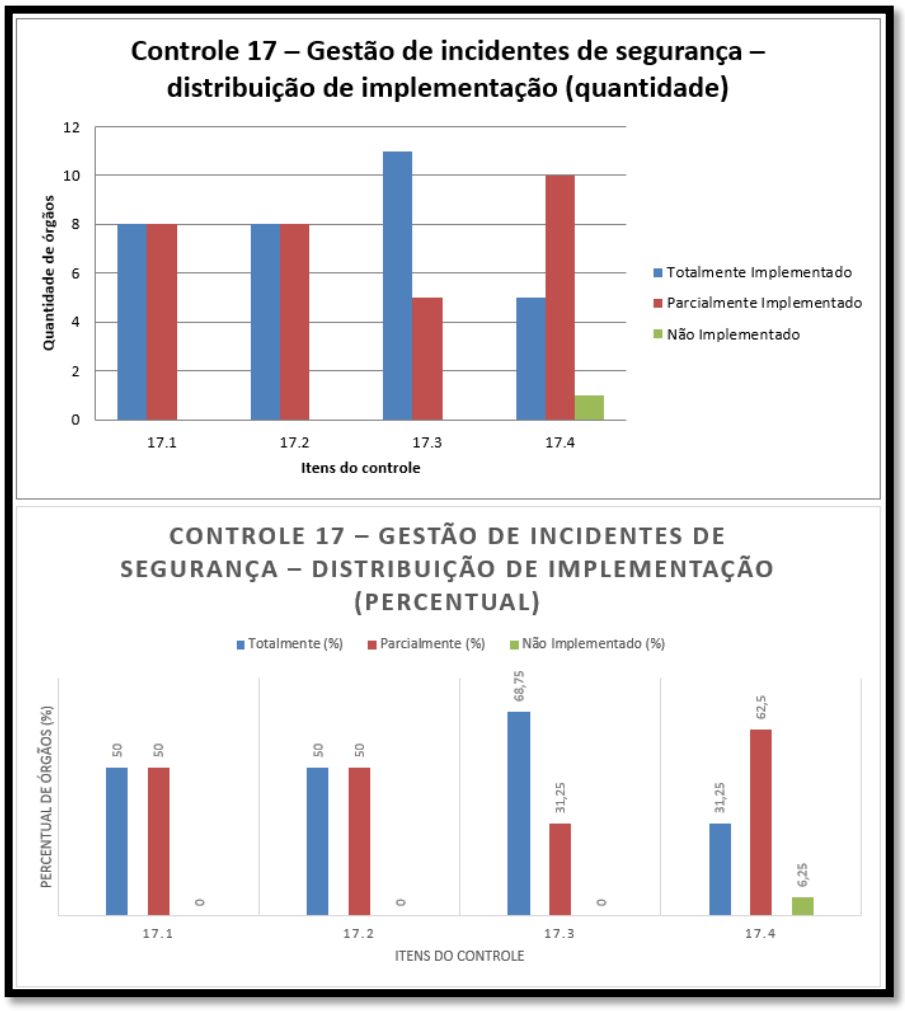
4.3.1 Controle 17 – Gestão de incidentes de segurança

Os resultados relativos ao Controle 17 indicam que a maioria dos órgãos já dispõe de algum nível de formalização na gestão de incidentes. A existência de um processo estruturado de gestão de incidentes é classificada como totalmente implementada por 50,0% dos órgãos (8 de 16), enquanto os outros 50,0% (8 de 16) relatam implementação parcial. Situação idêntica é observada na classificação e priorização de incidentes com base em impacto potencial, também com 50,0% de implementação total e 50,0% parcial.

A capacidade de responder aos incidentes de forma oportuna e eficaz apresenta desempenho ligeiramente melhor: 68,8% dos órgãos (11 de 16) indicam implementação total e 31,2% (5 de 16) implementação parcial. No entanto, ao se analisar o teste periódico do processo de resposta a incidentes, o cenário mostra fragilidades significativas: 62,5% dos órgãos (10 de 16) afirmam testar apenas de forma parcial, 31,2% (5 de 16) indicam testes totalmente implementados e 6,2% (1 de 16) não realizam testes.

Esses dados revelam que, embora os processos básicos de gestão de incidentes estejam presentes na maior parte dos órgãos da amostra, a etapa de validação por meio de testes estruturados ainda é um ponto fraco, o que limita a previsibilidade e a eficácia da resposta em cenários de crise.

Figura 6: Controle 17 – Gestão de incidentes de segurança



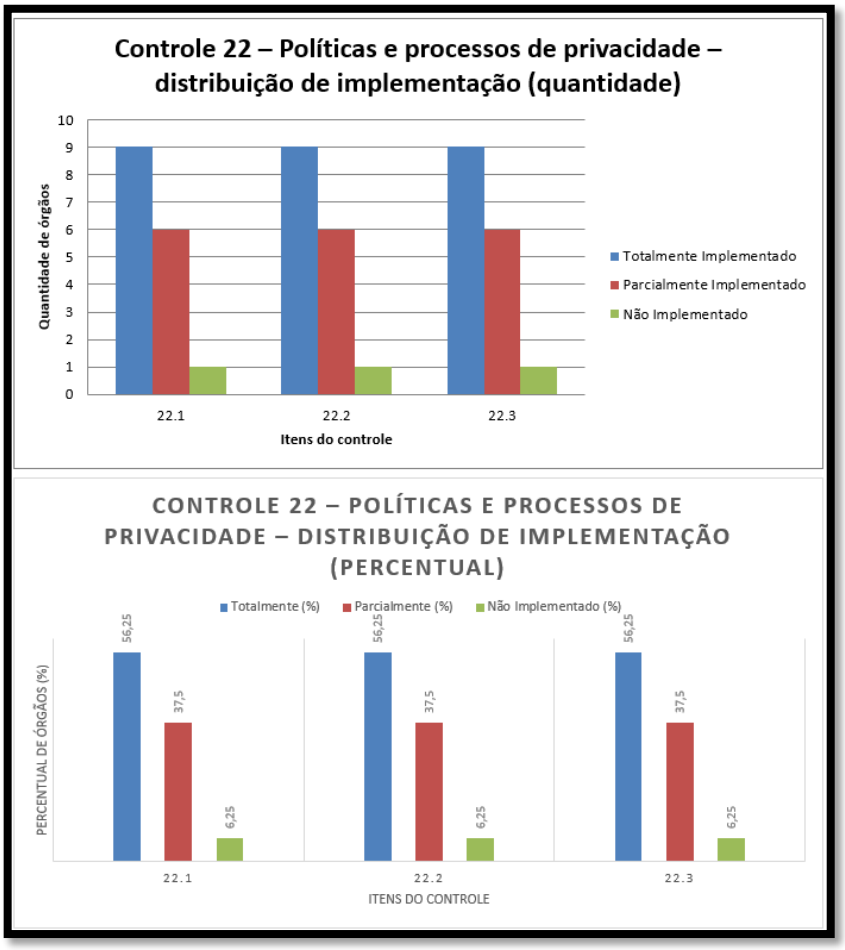
Fonte: Elaborado pelo autor (2025)

4.3.2 Controle 22 – Políticas e processos de privacidade

No âmbito da privacidade, os controles avaliados dizem respeito ao desenvolvimento e publicação de políticas de privacidade, à existência de processos de gestão de privacidade e à manutenção de procedimentos para facilitar o exercício de direitos de titulares. Em todos esses itens, observa-se um padrão semelhante: 56,2% dos órgãos (9 de 16) relatam implementação total, 37,5% (6 de 16) implementação parcial e 6,2% (1 de 16) não possuem o controle implementado.

Esse resultado indica que a maior parte dos órgãos da amostra já internalizou, ao menos parcialmente, as exigências associadas à proteção de dados e à transparência com os titulares. Entretanto, a presença de uma parcela ainda sem políticas ou processos minimamente estruturados sugere heterogeneidade na maturidade de privacidade dentro do conjunto analisado.

Figura 7: Controle 22 – Políticas e processos de privacidade



Fonte: Elaborado pelo autor (2025)

4.3.3 Eficácia dos processos, confiança na recuperação e testes práticos

A avaliação global da eficácia dos processos reforça a percepção de que há espaço para consolidação e melhoria. Para 62,5% das respostas (10 de 16), os processos são “definidos e funcionais”: existem, são conhecidos e utilizados, ainda que com algum grau de burocracia ou falta de integração. Em 25,0% dos casos (4 de 16), os processos são vistos como “burocráticos ou de papel”, sugerindo desalinhamento entre o que está formalizado e a prática cotidiana. Apenas 6,2% dos órgãos (1 de 16) relatam processos “otimizados e claros”, amplamente conhecidos e melhorados continuamente, enquanto outros 6,2% (1 de 16) descrevem um cenário “inexistente ou caótico”. Essa percepção está associada às respostas à questão 16 do questionário (ver Anexo A).

No que diz respeito à confiança na capacidade de recuperação e resposta, a maioria dos órgãos se posiciona em um patamar intermediário: 56,2% (9 de 16) classifica sua confiança como “média”, indicando que existem planos, mas pouco testados e ainda dependentes de pessoas-chave. Outros 37,5% (6 de 16) consideram ter “alta” confiança, com planos documentados e testados de forma razoável, e apenas 6,2% (1 de 16) se percebe em um patamar de “muito alta” confiança, com planos testados, automatizados e equipes bem treinadas. Esses resultados decorrem das respostas à questão 20 do questionário (ver Anexo A).

Por fim, a frequência de testes práticos de continuidade e recuperação (como exercícios de DR ou simulações de ataque) mostra um quadro de baixa sistematização. Em 37,5% das respostas (6 de 16), os planos só são efetivamente testados quando ocorre um incidente real. Em 18,8% dos casos (3 de 16), nunca houve testes formais, e 12,5% (2 de 16) indicam que o tema não se aplica ou não é conhecido. Apenas uma minoria realiza testes periódicos: 12,5% dos órgãos (2 de 16) testam anualmente, 12,5% (2 de 16) semestralmente ou com maior frequência, e 6,2% (1 de 16) a cada dois anos ou mais. Esses achados estão vinculados às respostas à questão 21 do questionário (ver Anexo A).

Em conjunto, esses resultados evidenciam que há um núcleo de processos documentados e em funcionamento, tanto para incidentes quanto para privacidade, mas ainda com forte dependência de pessoas, baixa automação e pouca cultura de

teste sistemático. Isso limita a resiliência efetiva frente a eventos de maior impacto. A coexistência de processos formalmente instituídos com baixa validação prática também aparece como fragilidade recorrente na auditoria do TCU (2024) em órgãos do SISP, reforçando que a maturidade processual não se esgota na existência de normas, mas exige ciclos de teste, revisão e melhoria contínua.

Tabela 2 – Implementação dos controles de conscientização, incidentes e privacidade (14, 17, 22 e 23) na amostra em % de respostas.

Medida (Controle)	Totalmente impl.	Parcialmente impl.	Não impl.	Não se aplica
14.1 – Programa estruturado de conscientização em segurança da informação	56,2%	31,2%	12,5%	0,0%
14.2 – Treinamento da força de trabalho em responsabilidades de segurança	50,0%	37,5%	12,5%	0,0%
17.1 – Processo estruturado de gestão de incidentes	50,0%	50,0%	0,0%	0,0%
17.2 – Classificação/priorização de incidentes por impacto	50,0%	50,0%	0,0%	0,0%
17.3 – Capacidade de resposta oportuna e eficaz a incidentes	68,8%	31,2%	0,0%	0,0%
17.4 – Testes periódicos do processo de resposta a incidentes	31,2%	62,5%	6,2%	0,0%
22.1 – Políticas de privacidade desenvolvidas e publicadas	56,2%	37,5%	6,2%	0,0%
22.2 – Processos de gestão da privacidade estabelecidos	56,2%	37,5%	6,2%	0,0%
22.3 – Procedimentos para exercício de direitos de titulares	56,2%	37,5%	6,2%	0,0%
23.1 – Programa formal de conscientização em privacidade	56,2%	25,0%	18,8%	0,0%
23.2 – Treinamentos em privacidade e proteção de dados	56,2%	37,5%	6,2%	0,0%

Fonte: Elaborado pelo autor (2025)

4.4 Bloco Software livre – diretrizes institucionais e ecossistema de ferramentas

O uso de software livre nos órgãos integrantes do SISP apresenta-se como um componente relevante para a construção de ambientes resilientes, especialmente

diante das limitações orçamentárias e da necessidade de assegurar transparência, auditabilidade e flexibilidade tecnológica. Embora não exista uma diretriz completamente homogênea entre as instituições, os dados coletados indicam que a maior parte dos órgãos adota uma postura pragmática ou favorável ao uso de soluções abertas, optando por ferramentas livres quando estas atendem aos requisitos funcionais e de segurança. Esse cenário reflete a adoção gradual de ecossistemas maduros de software livre, que incluem desde sistemas operacionais e bancos de dados até soluções de monitoramento, observabilidade, gestão de chamados e ferramentas de proteção cibernética. Além de reduzir custos recorrentes associados à aquisição de licenças, o uso de software livre permite maior autonomia na customização e na integração com sistemas legados, amplia a capacidade de auditoria do código e fortalece a colaboração entre órgãos, que podem compartilhar conhecimento técnico, experiências de implantação e boas práticas. Nesse sentido, observa-se que o software livre contribui não apenas como alternativa tecnológica, mas como vetor de fortalecimento da capacidade de resiliência cibernética e de otimização de recursos, alinhado às diretrizes sustentáveis de inovação na Administração Pública Federal.

4.4.1 Diretrizes institucionais para software livre (open source)

A maior parte dos órgãos adota uma postura pragmática em relação ao uso de software livre. Entre as respostas válidas, 53,3% dos órgãos (8 de 15) descrevem sua diretriz como “neutra/pragmática”, isto é, a escolha entre soluções livres ou proprietárias é feita caso a caso, sem preferência explícita. Outros 26,7% (4 de 15) declaram uma postura “favorável”, em que o uso de software livre é incentivado e amplamente adotado, embora não obrigatório. Há ainda 13,3% de respostas (2 de 15) que caracterizam a diretriz como “prioritária”, estabelecendo o software livre como primeira opção mandatória ou estratégica, e 6,7% (1 de 15) que indicam uma visão “restritiva”, com preferência por software proprietário e uso de software livre apenas como exceção. Esses resultados decorrem das respostas à questão 23 do questionário (ver Anexo A).

Esse quadro indica que o software livre é, em geral, bem aceito no contexto dos órgãos analisados, com predominância de abordagens pragmáticas ou

favoráveis, e apenas casos pontuais de preferência explícita por soluções proprietárias.

4.4.2 Principais softwares livres (open source) utilizados

Nas respostas abertas sobre os principais softwares livres utilizados em infraestrutura ou segurança, observa-se um ecossistema bastante rico, cobrindo desde sistemas operacionais até ferramentas especializadas de monitoramento, gestão e segurança. Entre os itens mais frequentes, destacam-se distribuições GNU/Linux (como Debian, Ubuntu Server e Oracle Linux) e bancos de dados livres (notadamente PostgreSQL e, em alguns casos, MySQL/MariaDB). As evidências desta subseção estão baseadas na questão 24 do questionário (ver Anexo A).

No campo de monitoramento e observabilidade, Zabbix e Wazuh aparecem de forma recorrente como soluções adotadas para monitoramento de infraestrutura, coleta de logs e detecção de ameaças. Também são mencionadas ferramentas associadas ao ecossistema ELK (Elastic, Logstash, Kibana), bem como Grafana e Graylog, compondo um panorama em que soluções de código aberto desempenham papel relevante na visibilidade operacional e de segurança.

Do ponto de vista de serviços de aplicação, são citados com frequência servidores web como Apache HTTP Server e Nginx, além de plataformas de atendimento e gestão de chamados, como GLPI e RT, e sistemas específicos como Moodle e QGIS. Em alguns casos, há menção ao uso de ferramentas de virtualização e orquestração abertas, como Proxmox e Docker, reforçando o papel do software livre como base da infraestrutura de TI.

De maneira geral, os dados evidenciam que, mesmo em órgãos cuja diretriz oficial é descrita como neutra, o software livre está amplamente presente em camadas críticas da infraestrutura e da segurança. Esse cenário sugere um potencial importante para iniciativas coordenadas de compartilhamento de boas práticas, padronização de arquiteturas e fortalecimento da resiliência cibernética a partir de um ecossistema comum de ferramentas abertas entre os órgãos integrantes do SISP analisados.

4.5 Bloco Maturidade e desafios – percepção global de resiliência cibernética

A análise integrada das respostas revela um quadro no qual os órgãos avaliados percebem possuir bases estruturadas de controles, processos e ferramentas, mas reconhecem também que a resiliência cibernética ainda encontra barreiras significativas para atingir níveis altos de maturidade sustentada. A totalidade dos respondentes posiciona sua instituição em níveis intermediários ou avançados de maturidade (Definido, Gerenciado ou Otimizado), o que indica que existe a consciência de que políticas e procedimentos estão estabelecidos e em operação.

Entretanto, diversos elementos mostram que essa maturidade, em muitos casos, permanece mais associada à existência formal de processos do que à comprovação sistemática de sua eficácia. A baixa frequência de testes de recuperação, o uso limitado de simulações de incidentes e o caráter moderadamente efetivo dos treinamentos apontam para lacunas entre a governança declarada e a capacidade operacional de responder de forma coordenada a crises reais. Esses desafios se agravam em contextos marcados por limitações de pessoal, recursos financeiros enxutos e dependência de sistemas legados, dificultando a evolução contínua dos controles e a institucionalização de melhorias.

Assim, a percepção global da resiliência cibernética da amostra indica avanços relevantes na implantação dos fundamentos exigidos pelo PPSI, mas reforça que a maturidade só será consolidada quando processos e capacidades forem validados rotineiramente por meio de exercícios, medições, auditorias e ciclos permanentes de aperfeiçoamento.

4.5.1 Percepção de maturidade em resiliência cibernética

Quando convidados a posicionar seu órgão em um nível de maturidade, nenhum dos participantes se identificou com estágios iniciais ou caóticos. A distribuição concentra-se em níveis intermediários e avançados: 43,8% das respostas (7 de 16) classificam a maturidade como “Definida”, ou seja, há processos documentados e aprovados, ainda que nem sempre seguidos ou medidos de forma sistemática. Outros 31,2% (5 de 16) se percebem no nível “Gerenciado”, com processos seguidos e monitorados por métricas, gerando ações de melhoria. Por fim, 25,0% (4 de 16) avaliam estar no nível “Otimizado”, em que os processos são

revisados e aperfeiçoados continuamente de forma proativa. Essa autoavaliação corresponde às respostas à questão 19 do questionário (ver Anexo A).

Esse padrão sugere uma percepção relativamente positiva por parte dos órgãos integrantes do SISP que compõem a amostra, com a totalidade dos participantes se posicionando em níveis em que há, ao menos, processos definidos. Ao mesmo tempo, a parcela ainda reduzida de órgãos que se enxergam como efetivamente “otimizados” indica consciência de que há espaço significativo para evolução. Quando comparado à auditoria do TCU (2024), que aponta que a maioria das organizações avaliadas no âmbito do SISP ainda não atinge plenamente o grupo de implementação básico (IG1) dos CIS Controls, esse quadro de autoavaliação sugere assimetria entre a percepção interna de maturidade e diagnósticos externos baseados em evidências documentais e testes, o que reforça a necessidade de aprofundar mecanismos objetivos de medição.

Tabela 3 – Síntese das percepções institucionais sobre ferramentas, fator humano, maturidade e software livre (em % de respostas).

Dimensão avaliada	Categoria	Percentual (%)
Suficiência das ferramentas	Básicas, com lacunas	25,0%
Suficiência das ferramentas	Suficientes	68,8%
Suficiência das ferramentas	Excedem (robustas)	6,2%
Percepção do fator humano	Usuários conscientes	56,2%
Percepção do fator humano	Usuários reativos	31,2%
Percepção do fator humano	Aliados proativos	12,5%
Efetividade dos treinamentos	Moderadamente efetivos	81,2%
Efetividade dos treinamentos	Muito efetivos	12,5%
Efetividade dos treinamentos	Inefetivos ou inexistentes	6,2%
Maturidade percebida	Definido	43,8%
Maturidade percebida	Gerenciado	31,2%
Maturidade percebida	Otimizado	25,0%
Confiança na recuperação	Média	56,2%
Confiança na recuperação	Alta	37,5%

Confiança na recuperação	Muito alta	6,2%
Diretriz de software livre	Neutra / pragmática	53,3%
Diretriz de software livre	Favorável	26,7%
Diretriz de software livre	Prioritária	13,3%
Diretriz de software livre	Restritiva	6,7%

Fonte: Elaborado pelo autor (2025)

4.5.2 Principais desafios enfrentados pelos órgãos participantes

A análise das respostas abertas referentes ao “principal desafio” enfrentado pelos órgãos integrantes do SISP foi conduzida por meio de análise de conteúdo temática (BARDIN, 2011), o que permitiu identificar padrões recorrentes nas falas dos participantes. A partir desse processo de categorização, os desafios foram agrupados em três eixos centrais: (I) limitações de recursos humanos e financeiros; (II) aspectos relacionados à conscientização e ao engajamento institucional; e (III) complexidade do ambiente tecnológico, em função da presença de múltiplos sistemas legados. Essa síntese decorre das respostas à questão 22 do questionário (ver Anexo A).

Em primeiro lugar, destaca-se a insuficiência de recursos humanos e financeiros. Em grande parte das respostas, os participantes mencionam explicitamente a falta de equipe dedicada à segurança da informação e à privacidade, a sobrecarga de profissionais que acumulam múltiplas funções e a dificuldade de contratar ou manter especialistas na área. Essa carência é frequentemente associada à indisponibilidade ou à limitação de orçamento específico para segurança cibernética, o que restringe a aquisição de ferramentas adequadas, a contratação de serviços especializados e a implantação de iniciativas contínuas de monitoramento, capacitação e melhoria de processos. Nesse contexto, muitos órgãos acabam concentrando esforços em ações reativas e pontuais, em detrimento de uma atuação planejada e sistemática.

Um segundo eixo de desafios diz respeito à conscientização e ao engajamento da força de trabalho e da alta gestão. Diversos respondentes relatam dificuldades para sensibilizar os servidores sobre a importância do cumprimento de políticas, normas e boas práticas de segurança e privacidade, bem como para assegurar a participação efetiva em treinamentos e ações de conscientização. Em vários casos, é apontada a

necessidade de maior envolvimento da alta administração, tanto no patrocínio das iniciativas de segurança quanto na priorização do tema na agenda institucional. Essa combinação de baixa conscientização e apoio limitado da gestão superior contribui para manter o fator humano em uma postura predominantemente reativa, o que fragiliza a resiliência organizacional frente a incidentes.

Por fim, verifica-se a influência da complexidade do ambiente tecnológico e da dependência de sistemas legados. Algumas respostas destacam que a infraestrutura de TI é formada por aplicações antigas, por vezes críticas para o negócio, que não foram originalmente concebidas com os requisitos atuais de segurança e privacidade. Essa realidade dificulta a aplicação de correções, a integração com ferramentas modernas de monitoramento e resposta a incidentes e a adoção de arquiteturas mais resilientes. Em cenários marcados por restrições de pessoal e orçamento, a necessidade de manter sistemas legados em operação prolonga a exposição a vulnerabilidades e torna mais lenta a evolução para modelos de maior maturidade em resiliência cibernética.

Os desafios relatados convergem para três grandes eixos: restrições de pessoal e orçamento, necessidade de maior conscientização e apoio da alta gestão e complexidade e criticidade da infraestrutura tecnológica. Esses elementos ajudam a explicar, em parte, por que controles e processos que aparecem como “parcialmente implementados” não avançam para níveis mais elevados de maturidade, indicando que a superação das fragilidades identificadas exige uma abordagem integrada que articule pessoas, processos e tecnologia nos órgãos integrantes do SISP. Os eixos identificados dialogam com discussões sobre governança digital e capacidade estatal no Brasil (RODRIGUES; CAMMAROSANO, 2022) e com os achados da auditoria do TCU (2024), que também apontam carências de recursos, baixa prioridade estratégica e complexidade tecnológica como fatores limitadores da maturidade em segurança da informação na Administração Pública Federal.

5 Conclusão

O presente estudo teve como objetivo analisar a resiliência cibernética em uma amostra de órgãos integrantes do SISP, utilizando o PPSI como principal referência. A partir da aplicação de um questionário estruturado, foi possível diagnosticar o grau

de aderência a controles considerados fundamentais, bem como levantar percepções sobre maturidade, eficácia de processos e principais desafios enfrentados na prática pelos times de TI, segurança da informação e privacidade. Embora a amostra de 16 respondentes represente uma fração reduzida do universo de órgãos integrantes do SISP, os resultados permitem compor um panorama inicial consistente sobre tendências e fragilidades recorrentes.

Os achados indicam a existência de uma base relevante de proteção já instalada. Rotinas de backup de dados essenciais, segmentação de rede e uso de mecanismos de prevenção de intrusão apresentam boa aderência, e a maioria dos órgãos percebe seu conjunto de ferramentas como “suficiente” para assegurar uma proteção básica. Ao mesmo tempo, surgem lacunas consistentes em pontos específicos, como a desativação da execução automática de mídias removíveis e o bloqueio de portas USB (medidas que, do ponto de vista técnico, são relativamente simples de implantar, mas que, na prática, esbarram em cultura organizacional e na necessidade de exceções), o uso mais avançado de filtragem em camada de aplicação e a centralização plena da gestão antimalware, todos com impacto direto na capacidade de resistir e se recuperar de incidentes.

O conjunto de respostas evidencia também que a resiliência não depende apenas da presença de ferramentas e controles, mas de como são apropriados pelas pessoas e sustentados por processos maduros. A maior parte dos órgãos relata possuir programas de conscientização e treinamento, além de processos formais de gestão de incidentes e de privacidade. Entretanto, esses mecanismos são frequentemente percebidos como moderadamente efetivos; muitos usuários ainda se comportam de forma mais reativa do que proativa, e diversos processos são vistos como burocráticos e pouco testados na prática. Testes estruturados de recuperação de backup, exercícios de resposta a incidentes e simulações de continuidade ainda ocorrem com baixa frequência, o que fragiliza a confiança real na capacidade institucional de suportar e contornar cenários mais críticos.

A autoavaliação de maturidade concentra todos os órgãos entre os níveis “Definido”, “Gerenciado” e “Otimizado”, com predominância dos dois primeiros. Esse padrão revela uma percepção relativamente positiva: os respondentes reconhecem a existência de políticas, processos e controles em funcionamento, mas também

admitem que ainda há um caminho importante a percorrer. Como os dados são autodeclaratórios e os testes práticos de continuidade e resposta a incidentes são pouco frequentes, essa confiança precisa ser interpretada com cautela, reforçando a importância de validar, na prática, a capacidade de resposta e recuperação, e não apenas a existência formal de documentos e controles.

As respostas abertas ajudam a explicar por que muitas iniciativas permanecem em estágio “parcialmente implementado” e não avançam para níveis mais altos de resiliência. Aparecem de forma recorrente a falta de equipe e de orçamento, a dificuldade de engajar usuários e alta gestão e a dependência de sistemas legados complexos. Esses fatores limitam a capacidade de evoluir de forma contínua, tanto na melhoria da infraestrutura quanto no amadurecimento de processos e da cultura de segurança. Em síntese, há consciência de que incidentes são inevitáveis, mas nem sempre há condições reais de reservar tempo, pessoas e recursos para treinar, testar e aprimorar a capacidade de resposta.

O estudo apresenta limitações, como o tamanho reduzido da amostra, o caráter autodeclaratório das informações e o recorte em um único momento no tempo. Ainda assim, os objetivos propostos foram alcançados. O trabalho oferece um retrato realista de onde esses órgãos já avançaram e onde ainda patinam em resiliência cibernética, ao evidenciar que a mera presença de controles não se traduz automaticamente em capacidade consolidada de resistir, responder e recuperar. Ao dialogar com diagnósticos mais amplos, como o do Tribunal de Contas da União sobre o PPSI, o estudo contribui para detalhar como a baixa maturidade se manifesta no cotidiano das instituições e reforça a necessidade de fortalecer a governança, a responsabilidade da alta administração sobre riscos cibernéticos e a construção de capacidades efetivas de resposta e recuperação, para além da conformidade formal com checklists de controles.

Como próximos passos, pretende-se ampliar o alcance do estudo por meio da aplicação do questionário a todos os órgãos integrantes do SISP, de forma a obter uma visão mais abrangente e representativa da resiliência cibernética na Administração Pública Federal. Pretende-se também a melhoria do instrumento de coleta com a inclusão de um bloco específico de caracterização institucional e do respondente, contemplando questões sobre o tipo de órgão (Ministério, Autarquia,

Fundação, Agência reguladora ou outro órgão integrante do SISP), o porte aproximado em número de servidores e colaboradores, o papel principal do respondente em TIC, segurança ou privacidade (gestão, técnico, consultivo ou outro) e a existência de unidade ou equipe formalmente designada para segurança da informação e privacidade (sim, parcialmente ou não). Essas sugestões encontram-se sistematizadas no Anexo B, sob a forma de um conjunto adicional de questões (Q1 a Q4), e visam permitir análises futuras mais refinadas, correlacionando o grau de implementação dos controles do PPSI, o perfil institucional e a estrutura dedicada ao tema.

REFERÊNCIAS

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2016.

CASA CIVIL. Presidência da República. **Decreto nº 12.573**, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança – E-Ciber. Diário Oficial da União, Brasília, DF, 5 ago. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Decreto/D12573.htm. Acesso em: 18 nov. 2025.

CASA CIVIL. Presidência da República. **Decreto nº 7.579**, de 11 de outubro de 2011. Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, do Poder Executivo federal. Diário Oficial da União, Brasília, DF, 13 out. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7579.htm. Acesso em: 18 nov. 2025.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

IBM SECURITY. **Cost of a Data Breach Report 2024**. Armonk, NY: IBM Corporation, 2024. Disponível em: https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report. Acesso em: 20 nov. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27001:2022 – **Information security, cybersecurity and privacy protection** – Information security management systems – Requirements. Geneva: ISO; IEC, 2022. Disponível em: https://www.iso.org/standard/82875.html. Acesso em: 20 nov. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27002:2022 – **Information security,**

cybersecurity and privacy protection – Information security controls. Geneva: ISO; IEC, 2022. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: 20 nov. 2025.

MGI. Ministério da Gestão e da Inovação em Serviços Públicos. **75% dos órgãos federais entregam autodiagnóstico e plano de trabalho voltado para privacidade e segurança da informação**. Brasília, DF, 15 ago. 2025. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/agosto/75-dos-orgaos-federais-entregam-autodiagnostico-e-plano-de-trabalho-voltado-para-privacidade-e-seguranca-da-informacao. Acesso em: 23 nov. 2025.

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento**: pesquisa qualitativa em saúde. 15. ed. São Paulo: Hucitec, 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The NIST Cybersecurity Framework (CSF) 2.0**. Gaithersburg, MD: NIST, 2024. (NIST CSWP 29). Disponível em: https://doi.org/10.6028/NIST.CSWP.29. Acesso em: 20 nov. 2025.

PPSI. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Programa de Privacidade e Segurança da Informação (PPSI): **framework de privacidade e segurança da informação**. Brasília, DF, 2025. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos. Acesso em: 18 nov. 2025.

RODRIGUES, Cristina Barbosa; CAMMAROSANO, Flávia Giorgini Fusco. **Governança Digital**: Avanços e Desafios do Processo Administrativo Eletrônico no Brasil. Revista de Direito Internacional e Globalização Econômica, São Paulo, v. 9, n. 9, p. 198-219, 2022. DOI: 10.23925/2526-6284/2022.v9n9.58939. Disponível em: https://revistas.pucsp.br/index.php/DIGE/article/view/58939. Acesso em: 20 nov. 2025.

SGD/MGI. Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos. **Linha do tempo**: do Eletrônico ao Digital. Brasília, DF, 25 nov. 2019. Atualizado em: 5 set. 2024. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital. Acesso em: 20 nov. 2025.

SGD/MGI. Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos. **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, 30 mar. 2023. Seção 1, p. 92. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 18 nov. 2025.

TCU. Tribunal de Contas da União. **Acórdão nº 2387/2024** – Segurança da informação na Administração Pública Federal. Brasília, DF: TCU, 2024. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A2387%2520ANOACORDAO%253A2024%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acesso em: 18 nov. 2025.

VERIZON. 2024 **Data Breach Investigations Report**. 17. ed. New York: Verizon, 2024. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 20 nov. 2025.

ANEXO A – Instrumento de pesquisa: Questionário sobre resiliência cibernética e PPSI

O formulário de pesquisa foi implementado na plataforma Microsoft Forms e aplicado a profissionais que atuam em unidades de TIC, segurança da informação ou privacidade em órgãos integrantes do SISP. O instrumento é anônimo e tem como objetivo verificar o nível de implementação de controles e medidas de resiliência cibernética, bem como captar percepções sobre processos, maturidade e desafios, para subsidiar o artigo " Resiliência cibernética em órgãos do SISP: diagnóstico de controles selecionados do PPSI". As questões 1 a 7 subsidiam principalmente as análises apresentadas nas subseções 4.1 a 4.4; as questões 8 a 18 relacionam-se à discussão sobre o fator humano, processos de privacidade, gestão de incidentes e continuidade (subseções 4.5 e 4.6); e as questões 19 a 24 fundamentam as análises de maturidade percebida, principais desafios e uso de software livre (subseções 4.7 e 4.8). A seguir, apresenta-se o conteúdo integral do questionário utilizado no estudo.

Instruções gerais e escala de avaliação

Este questionário leva cerca de 15 minutos para ser concluído. O objetivo é verificar o nível de implementação dos controles e das medidas de resiliência cibernética na organização. As respostas consolidadas e anônimas são utilizadas exclusivamente para fins de pesquisa. Para as questões que avaliam medidas dos controles do PPSI, utiliza-se a seguinte escala:

- Totalmente Implementado: a medida está formalmente documentada, implementada e é seguida de forma consistente.

- Parcialmente Implementado: a medida existe, mas é aplicada de forma inconsistente, não está totalmente documentada ou não cobre todo o escopo necessário.

- Não Implementado: a medida não existe ou não é executada.

- Não se Aplica: a medida não é relevante para o escopo daquela área ou processo.

1. Controle 10 – Defesas contra Malware*

Avalie o nível de implementação das seguintes medidas para o Controle 10, utilizando a escala: Totalmente Implementado / Parcialmente Implementado / Não Implementado / Não se Aplica.

10.1: Implementar e manter defesas contra malware nos ativos da organização.

10.2: O órgão configura atualizações automáticas de assinatura antimalware?

10.3: O órgão desabilita a execução e reprodução automática para mídias removíveis?

10.5: O órgão gerencia o software antimalware de maneira centralizada?

2. Justificativas para o Controle 10

Campo aberto para o respondente citar ferramentas (por exemplo, antivírus, EDR), políticas internas ou motivos específicos para as avaliações "Parcialmente Implementado" ou "Não Implementado" registradas no Controle 10.

3. Controle 11 – Recuperação de Dados*

Avalie o nível de implementação das seguintes medidas para o Controle 11, utilizando a escala: Totalmente Implementado / Parcialmente Implementado / Não Implementado / Não se Aplica.

11.1: Estabelecer e manter um processo de recuperação de dados.

11.2: Realizar backups das informações necessárias para a continuidade dos serviços essenciais.

11.3: Proteger os dados de backup contra acesso não autorizado, modificação e destruição.

11.4: Testar periodicamente a capacidade de recuperação dos dados de backup.

4. Justificativas para o Controle 11

Campo aberto para o respondente citar ferramentas (por exemplo, Veeam, Bacula), políticas (por exemplo, códigos de políticas de backup), frequência de testes ou outros comentários relacionados ao Controle 11.

5. Controle 13 – Monitoramento e Defesa da Rede*

Avalie o nível de implementação das seguintes medidas para o Controle 13, utilizando a escala: Totalmente Implementado / Parcialmente Implementado / Não Implementado / Não se Aplica.

13.1: O órgão realiza filtragem de tráfego entre os segmentos de rede?

13.4: O órgão implanta soluções para prevenção de intrusão de rede?

13.5: O órgão implanta controle de acesso em nível de porta?

13.6: O órgão realiza filtragem em camada de aplicação?
13.7: O órgão centraliza alertas de eventos de segurança?

6. Justificativas para o Controle 13

Campo aberto para o respondente citar ferramentas (por exemplo, firewalls, SIEM, Splunk), processos de análise de logs ou outros comentários relativos à defesa e ao monitoramento da rede.

7. Suficiência das Ferramentas*

Questão de percepção sobre o pilar Tecnologia (antivírus, firewalls, backups, monitoramento etc.). O respondente escolhe a opção que melhor representa a adequação e a suficiência do conjunto de ferramentas de segurança disponível na instituição:

- Excedem (Robustas): temos ferramentas avançadas, integradas e que cobrem os principais riscos de forma proativa.

- Suficientes (Adequadas): temos o necessário para operar e garantir a resiliência básica, embora possam faltar algumas integrações.

- Básicas (Com Lacunas): temos o mínimo, mas faltam ferramentas importantes ou muitas estão obsoletas, exigindo esforço manual.

- Insuficientes (Críticas): as ferramentas são muito fracas ou desatualizadas, representando risco claro para a operação.

- Não sei avaliar.

8. Controle 14 – Conscientização e Treinamento (Segurança)*

Avalie o nível de implementação das seguintes medidas para o Controle 14, utilizando a escala: Totalmente Implementado / Parcialmente Implementado / Não Implementado / Não se Aplica.

14.1: Estabelecer e manter um programa de conscientização em segurança da informação.

14.2: Treinar a força de trabalho sobre suas responsabilidades em segurança da informação.

9. Justificativas para o Controle 14

Campo aberto para o respondente citar plataformas de treinamento (por exemplo, Moodle), frequência de campanhas, ações de comunicação e outros comentários relacionados à conscientização em segurança.

10. Percepção do Fator Humano (o "Firewall Humano”) *

Questão de percepção sobre o comportamento geral de colaboradores e gestores em relação à segurança e privacidade. As opções de resposta são:

- Aliados (Proativos): são vigilantes, questionam e-mails suspeitos, reportam incidentes ativamente e entendem seu papel na defesa.

- Conscientes (Cuidadosos): entendem os riscos básicos e tentam seguir as políticas, mas não são proativos na detecção.

- Reativos (Seguem o Básico): só se preocupam com segurança quando obrigados, cobrados ou após um incidente.

- Desatentos (Vulneráveis): frequentemente ignoram regras por conveniência, clicam em links suspeitos ou usam senhas fracas.

- Não sei avaliar.

11. Efetividade dos Treinamentos*

Questão de percepção sobre a efetividade dos treinamentos e campanhas de conscientização (controles 14 e 23) em melhorar a maturidade de segurança. As opções de resposta são:

- Muito efetivos: há melhora clara e sustentada na cultura e no comportamento.

- Moderadamente efetivos: há aumento de atenção por um tempo, mas os velhos hábitos retornam rapidamente.

- Pouco efetivos / burocráticos: vistos apenas como obrigação formal, sem mudança real no dia a dia.

- Inefetivos ou inexistentes: não há treinamentos relevantes ou eles não abordam os riscos reais.

- Não sei avaliar / não participei.

12. Controle 17 – Gestão de Resposta a Incidentes*

Avalie o nível de implementação das seguintes medidas para o Controle 17, utilizando a escala: Totalmente Implementado / Parcialmente Implementado / Não Implementado / Não se Aplica.

17.1: Estabelecer e manter um processo de gestão de incidentes de segurança.

17.2: Classificar e priorizar os incidentes de segurança com base em seu impacto potencial.

17.3: Responder aos incidentes de segurança de forma oportuna e eficaz.
17.4: Testar o processo de resposta a incidentes de segurança periodicamente.

13. Justificativas para o Controle 17

Campo aberto para o respondente citar documentos (por exemplo, Plano de Resposta a Incidentes), ferramentas de gestão (por exemplo, GLPI, ServiceNow) ou datas dos últimos testes realizados.

14. Controle 22 – Políticas e Processos (Privacidade)*

Avalie o nível de implementação das seguintes medidas para o Controle 22, utilizando a escala: Totalmente Implementado / Parcialmente Implementado / Não Implementado / Não se Aplica.

22.1: Desenvolver e publicar a(s) política(s) de privacidade.

22.2: Estabelecer e manter processos para a gestão da privacidade.

22.3: Estabelecer e manter procedimentos para facilitar o exercício dos direitos dos titulares.

15. Justificativas para o Controle 22

Campo aberto para o respondente citar documentos de política, nomes de processos e ferramentas de gestão da privacidade.

16. Eficácia dos Processos*

Questão de percepção sobre a clareza e a eficácia dos processos (gestão de incidentes, políticas de privacidade, procedimentos etc.). As opções de resposta são:

- Otimizados e claros: processos conhecidos, integrados, eficazes e melhorados ativamente.

- Definidos e funcionais: processos documentados que geralmente funcionam, ainda que com alguma burocracia.

- Burocráticos / "de papel": existem formalmente, mas são confusos, desatualizados ou pouco seguidos na prática.

- Inexistentes / caóticos: não há processos formais claros ou eles são contraditórios.

- Não sei avaliar.

17. Controle 23 – Conscientização e Treinamento (Privacidade)*

Avalie o nível de implementação das seguintes medidas para o Controle 23, utilizando a escala: Totalmente Implementado / Parcialmente Implementado / Não Implementado / Não se Aplica.

23.1: Estabelecer e manter um programa de conscientização em privacidade e proteção de dados.

23.2: Treinar a força de trabalho em privacidade e proteção de dados.

18. Justificativas para o Controle 23

Campo aberto para o respondente citar nomes de treinamentos (por exemplo, "Treinamento LGPD"), plataformas utilizadas e datas ou frequência de aplicação.

19. Percepção de Maturidade*

Questão de autoavaliação do nível de maturidade geral em resiliência cibernética da instituição. As opções são:

- Inicial / ad hoc: atuação reativa, baseada em apagar incêndios e esforço individual.

- Definido: processos documentados e aprovados, ainda que nem sempre seguidos ou medidos.

- Gerenciado: processos seguidos, medidos com métricas e com ações de melhoria baseadas nesses dados.

- Otimizado: processos revisados e melhorados continuamente, de forma proativa.

- Não sei avaliar.

20. Confiança na Recuperação (Capacidade de Resposta)*

Questão de percepção sobre o nível de confiança na capacidade da instituição de restabelecer os serviços essenciais diante de um incidente cibernético grave ou de um desastre. As opções são:

- Muito alta: há planos testados, automatizados e equipes treinadas.

- Alta: há planos documentados e testados de forma razoável.

- Média: existem planos, mas pouco testados e dependentes de pessoas chave.

- Baixa: planos inexistentes ou desatualizados.

- Nula / não sei avaliar.

21. Validação Prática (Testes de DR/Ataques)*

Questão sobre a frequência com que o Plano de Recuperação de Desastres (PRD) ou o Plano de Resposta a Incidentes (PRI) é testado na prática, por meio de simulações de ataque, exercícios de mesa ou testes de failover. As opções são

- Semestralmente ou mais frequentemente.

- Anualmente.

- A cada 2 anos ou mais.

- Apenas quando ocorre um incidente real.

- Nunca foram testados formalmente.

- Não se aplica / não sei.

22. Principal Desafio*

Questão aberta na qual o respondente descreve, em suas próprias palavras, qual é o maior desafio ou ponto mais vulnerável da instituição hoje para o avanço da

resiliência cibernética (por exemplo, falta de orçamento, falta de pessoal, dificuldade de conscientizar a alta gestão, sistemas legados etc.).

23. Diretriz institucional quanto à adoção de software livre (open source)*

Questão de percepção sobre a diretriz institucional em relação ao uso de software livre, com as seguintes opções:

- Prioritária: o uso de software livre é a primeira opção mandatória ou estratégica.

- Favorável: o uso é incentivado e amplamente adotado, mas não obrigatório.

- Neutra / pragmática: escolhe-se a melhor ferramenta (livre ou proprietária) caso a caso, sem preferência prévia.

- Restritiva: há preferência por software proprietário/comercial; software livre é exceção.

- Proibitiva: o uso de software livre não é permitido ou é extremamente burocrático.

24. Principais softwares livres utilizados na infraestrutura ou segurança*

Questão aberta solicitando que o respondente liste os principais softwares livres utilizados na infraestrutura ou na segurança da instituição, como sistemas operacionais GNU/Linux (por exemplo, Debian, Ubuntu Server), bancos de dados livres (por exemplo, PostgreSQL, MariaDB), servidores web (por exemplo, Apache, Nginx), ferramentas de monitoramento e segurança (por exemplo, Zabbix, Wazuh) e outras soluções críticas de código aberto.

ANEXO B – Proposta de aprimoramento do instrumento de pesquisa

Este anexo apresenta um conjunto de questões adicionais sugeridas para aperfeiçoar o instrumento de pesquisa em ciclos futuros, com foco na caracterização institucional e do participante. O objetivo é permitir análises mais refinadas, correlacionando o grau de implementação dos controles do PPSI e a percepção de resiliência cibernética com o porte do órgão, o tipo de entidade, o perfil profissional e a existência de estruturas formais de segurança da informação e privacidade.

Q1. Tipo de órgão em que você atua: Ministério, Autarquia, Fundação, Agência reguladora ou outro órgão integrante do SISP.

Q2. Quantidade aproximada de servidores/colaboradores do órgão: até 200, 201–500, 501–2.000 ou acima de 2.000.

Q3. Papel principal do respondente em TIC/segurança/privacidade: Gestão, Técnico, consultivo ou outro.

Q4. Existe unidade ou equipe formalmente designada para segurança da informação/privacidade? Sim, parcialmente ou Não.