GRUPO I – CLASSE V – Plenário
TC 005.618/2025-8
Natureza: Monitoramento.
Unidades Jurisdicionadas: Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e outros.
Representação legal: não há.

SUMÁRIO: AUDITORIA OPERACIONAL. AVALIAÇÃO DOS CONTROLES DE CIBERSEGURANÇA E DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES DO SISP. ANÁLISE DE ADERÊNCIA A BOAS PRÁTICAS, EM ESPECIAL O FRAMEWORK DO PPSI. RISCOS DE ATAQUES CIBERNÉTICOS IDENTIFICADOS. IMPLEMENTAÇÃO DE MEDIDAS DE SEGURANÇA AQUÉM DO ESPERADO. PAPEL DA ALTA ADMINISTRAÇÃO NO GERENCIAMENTO DE RISCOS. RECOMENDAÇÕES. ARQUIVAMENTO. MONITORAMENTO. IMPLEMENTAÇÃO PARCIAL DAS RECOMENDAÇÕES. EXPEDIÇÃO DE NOVA RECOMENDAÇÃO. DETERMINAÇÃO PARA CONSTITUIÇÃO DE PROCESSO APARTADO PARA APURAÇÃO DE RESPONSABILIDADES. ENCERRAMENTO DESTE PROCESSO COM APENSAÇÃO À AUDITORIA OPERACIONAL MONITORADA.

RELATÓRIO

Transcrevo a seguir a instrução elaborada no âmbito da Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI), acostada à peça 443, com a qual se manifestou de acordo o corpo dirigente da unidade (peças 444 e 445):

"INTRODUÇÃO

1. *Trata-se de monitoramento de deliberações, de acordo com o previsto no art. 243 do Regimento Interno do Tribunal de Contas da União (RI/TCU) e no art. 4º, inciso III, da Portaria - Segecex 27/2009 (Padrões de Monitoramento). O monitoramento foi determinado pelo Plenário desta Corte no item 9.7 do Acórdão 2.387/2024-TCU-Plenário (Rel. Min. Augusto Nardes) (peça 6).*

HISTÓRICO

2. *Em 2024, o TCU, por meio da Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI), realizou fiscalização na modalidade Auditoria Operacional (TC 010.390/2024-3) com o seguinte objetivo (peça 3, p. 2):*

> *Avaliar em que medida os controles de cibersegurança e de segurança da informação implementados pelas organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) estão de acordo com as boas práticas, em especial comparados ao previsto no Framework de Privacidade e Segurança da Informação (Portaria-SGD/MGI 852/2023).*

3. *Em síntese, a fiscalização:*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

3.1. promoveu uma avaliação dos controles de cibersegurança nas organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), definindo como escopo os controles 1 a 18 do Framework de Privacidade e Segurança da Informação;

3.2. concluiu que as organizações do Sisp estão aquém do esperado no que se refere à implementação de medidas de segurança cibernética e que o PPSI é uma iniciativa promissora, com oportunidades de melhoria.

4. *Em decorrência dessa fiscalização, foi prolatado o Acórdão 2.387/2024-TCU-Plenário, com as seguintes deliberações:*

> *9.1. recomendar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) que aperfeiçoe o PPSI, gerenciando os riscos constantes do apêndice D do relatório de peça 200, adotando as medidas de controle que estiverem sob sua governabilidade e orientando as organizações do Sisp quando as medidas estiverem na respectiva esfera de governabilidade;*
>
> *9.2. recomendar a cada uma das organizações do Sisp relacionadas no apêndice E do relatório de peça 200 que:*
>
> *9.2.1. adotem medidas para implementar os controles de segurança cibernética necessários para reduzir o risco de ataques cibernéticos ao nível aceitável para as políticas públicas que executam, utilizando como referencial as diretrizes expedidas pela SGD/MGI por meio do PPSI, de acordo com o art. 8º da Portaria-SGD/MGI nº 852/2023;*
>
> *9.2.2. envidem esforços para que o processo de gestão de riscos decorrentes de ataques cibernéticos seja liderado explicitamente pela sua alta administração, alinhado ao previsto no art. 17 do Decreto nº 9.203/2017;*
>
> *9.3. dar ciência às 101 organizações que não responderam ao ciclo 3 do PPSI até o dia 14/8/2024 (lista no apêndice A do relatório de peça 200), com fundamento no disposto no art. 9º, I, da Resolução-TCU nº 315/2020, sobre a obrigatoriedade de enviar à SGD/MGI sua autoavaliação e plano de ação, nos prazos determinados por ela em cada ciclo de avaliação do PPSI, conforme disposto nos artigos 6º, III, 7º, I, e 8º, I, do Decreto nº 7.579/2011, c/c o disposto no art. 9º, §§ 1º e 2º, da Portaria SGD/MGI nº 852/2023;*

5. *O Hospital de Clínicas de Porto Alegre e a Agência Nacional de Transportes Terrestres (ANTT) opuseram embargos de declaração alegando equívoco na inclusão de seus nomes na lista das 101 organizações que não responderam ao ciclo 3 do PPSI até o dia 14/8/2024 (peça 10). Por meio do Acórdão 630/2025–TCU–Plenário (Rel. Min. Augusto Nardes), o Tribunal determinou à AudTI que suprimisse os nomes do hospital e da agência da relação das 101 organizações (peça 9).*

6. *O ministro relator em seu relatório (Acórdão 2.387/2024-TCU-Plenário) entendeu que (peça 8, p. 31):*

> *Considerando a relevância do risco, o monitoramento das recomendações propostas é fundamental, pois possibilita o acompanhamento da questão por parte do Tribunal. O monitoramento, a ser realizado por esta unidade técnica, caso as recomendações sejam aprovadas pelo relator e pelo Plenário do TCU, deverá iniciar-se o mais breve possível após a ciência do acórdão por parte dos órgãos envolvidos, mas levando em conta a conveniência e a oportunidade presentes à época.*
>
> *Especificamente quanto às recomendações às 254 organizações do Sisp, a unidade técnica deverá observar, além da conveniência e oportunidade, a forma mais eficiente de realizar seu monitoramento, dado o grande número de organizações. Poderá fazê-lo por*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

> *amostragem, no curso de outras ações de controle ou ainda por outra forma que se mostre mais eficiente que atuar em todas as 254 organizações.*

7. *Em 27/3/2026, por meio de análise realizada pela AudTI, propôs-se a realização de diligência à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI) para complementar os autos com informações que permitissem a análise de mérito sobre o atendimento das deliberações do Acórdão 2.387/2024-TCU-Plenário (peça 367, p. 4). Propôs-se, ainda, diligência ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) para que enviasse as respostas ao Autodiagnóstico da Política Nacional de Segurança da Informação que realizara no início de 2026, por entender que contribuiriam para avaliar a manutenção ou a retirada do tema Segurança da Informação e Cibernética da Lista de Alto Risco (LAR) do TCU (peça 367, p. 4).*

8. *As comunicações processuais pertinentes foram efetuadas: Ofício 10323/2026-TCU/Seproc (GSI, peça 378) e Ofício 11923/2026-TCU/Seproc (SGD/MGI, peça 382), com as devidas ciências dos destinatários (peças 380 e 383). Assim, as organizações encaminharam as informações solicitadas por esta unidade: GSI/PR (peças 384 a 386) e SGD/MGI (peças 393-394 e 417-420).*

9. *Destaca-se que o monitoramento do item 9.2.2 do Acórdão 2.387/2024-TCU-Plenário será realizado no próximo ciclo de monitoramento, visto que a informação necessária constará dos próximos levantamentos do PPSI.*

ANÁLISE DO ATENDIMENTO DAS DELIBERAÇÕES

Recomendação 9.1

> *9.1. recomendar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) que aperfeiçoe o PPSI, gerenciando os riscos constantes do apêndice D do relatório de peça 200, adotando as medidas de controle que estiverem sob sua governabilidade e orientando as organizações do Sisp quando as medidas estiverem na respectiva esfera de governabilidade;*

Situação que levou à proposição da deliberação

10. *A equipe de auditoria identificou e discutiu com os gestores da Secretaria a existência de riscos que, se gerenciados, transformar-se-iam em oportunidades de melhoria para o programa. Os riscos foram divididos em dois grupos: institucionalização e processo de implementação do programa (peça 3, p. 46), quais sejam:*

10.1. Institucionalização do programa

10.1.1. Insuficiência de indicadores e metas do programa (risco RRA1);

10.1.2. Ausência, na estrutura de governança do PPSI, de atribuição explícita de responsabilidade para a Alta Administração (AA) das organizações quanto à implementação do PPSI (risco RRA2);

10.1.3. Escala de medição das medidas de segurança possibilita que acima de 50% seja considerado como implementado totalmente (risco RRA3).

10.2. Implementação do programa

10.2.1. SGD/MGI apresenta limitação quantitativa em pessoal para as atividades do ciclo externo (risco RPE1);

10.2.2. Organizações do Sisp têm deficiências em pessoal (quantidade e/ou qualificação) para as atividades do ciclo interno (risco RPE2);

10.2.3. Em algumas organizações, existe uma rotatividade grande de pessoas no quadro (risco RPE3);

10.2.4. Ausência de designação do gestor de segurança da informação em 21% das organizações (risco RPE4);

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

10.2.5. A Comissão de Coordenação do Sisp não participa da seleção dos controles priorizados em cada ciclo (alinhado ao previsto no Decreto 7.579/2011, art. 4º, inciso II, c/c art. 5º, inciso I) (risco RPE5);

10.2.6. Ausência de informações (evidências) sobre a implementação dos controles, pois o PPSI é implementado por meio de autoavaliação (risco RIN1);

10.2.7. Ausência de agrupamento das organizações por tamanho, finalidade, similaridade ou outro critério possível (risco RPR2);

10.2.8. Ausência de mecanismo de cumprimento (enforcement) na implementação do framework pelas organizações do Sisp (risco RPR3);

10.2.9. Não há uma forma de pré-preenchimento com as respostas do ciclo anterior c/c mudança do modelo do instrumento a cada ciclo (risco RPR4);

10.2.10. Gestores das organizações desconhecem o modelo de três linhas de defesa, acreditando que o setor de Segurança Cibernética (SegCiber) da organização é o único responsável pela gestão de riscos de SegCiber (risco RPR5);

10.2.11. Insuficiência de recursos financeiros para implementação das medidas priorizadas nas organizações do Sisp (risco RRE1);

10.2.12. Ferramenta de acompanhamento da implementação do framework no formato de planilha eletrônica. Nem todas as organizações do Sisp possuem o Microsoft Excel para preencher o diagnóstico e o plano de trabalho (risco RTE1).

Providências adotadas pela SGD/MGI

11. *Em resposta ao Ofício 11923/2026-TCU/Seproc, a SGD/MGI enviou a Nota Técnica SEI 18707/2026/MGI contendo o tratamento dado aos riscos apontados pela equipe de auditoria (peça 394). De forma resumida, o tratamento adotado para todos os riscos foi a mitigação, tendo como evidências principais a Portaria - SGD/MGI 9.511/2025 e a Instrução Normativa - SGD/MGI 4/2026.*

Análise das providências

12. *O Programa de Privacidade e Segurança da Informação (PPSI), liderado pela SGD/MGI, era regido pela Portaria - SGD/MGI 852/2023 e sua abordagem ocorria por meio de ciclos avaliativos de 180 dias. De acordo com o item 13.2 da Nota Técnica 49451/2024/MGI (peça 365), o 5º ciclo do PPSI terminou em 31/12/2025. Após o início do ciclo 5 em 1º/7/2025, foi publicada a Portaria - SGD/MGI 9.511/2025, que instituiu o PPSI 2.0, com início previsto para entrar em vigor em 1º de janeiro de 2026. Dessa forma, a Portaria - SGD/MGI 852/2023 foi revogada. Nesse sentido, em 16/1/2026 foi publicada a Instrução Normativa - SGD/MGI 4/2026, que dispõe sobre o ciclo de implementação de 2026 do framework do PPSI 2.0.*

13. *Um dos documentos do PPSI 2.0 é o Guia do Framework de Privacidade e Segurança da Informação versão 1.2 (https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-2-30012026.pdf), que tem como objetivo fornecer informações de referência claras e abrangentes para apoiar e esclarecer os diversos aspectos relacionados à concepção, estruturação e implementação dos controles e medidas que compõem o framework.*

14. *A seguir, procede-se à análise das respostas da SGD/MGI para os riscos identificados pela equipe de auditoria:*

Risco RRA1 - Insuficiência de indicadores e metas do programa

Providências adotadas pela SGD/MGI (peça 394, p. 1)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

15. *A Secretaria afirma que incluiu previsão normativa acerca dos indicadores iBase, iSeg e iPriv na Instrução Normativa - SGD/MGI 4/2026. Ademais, afirma que a Estratégia Federal de Governo Digital (EFGD) - formalizada pelo Decreto 12.198, de 24 de setembro de 2024 e pela Portaria - SGD/MGI 6.618, de 25 de setembro de 2024 - estabelece princípios, objetivos e iniciativas para o aprimoramento da governança digital do Governo Federal. Nesse sentido, a iniciativa 9.1 da EFGD tem por objetivo incrementar o valor médio do índice de segurança da informação (iSeg) do Programa de Privacidade e Segurança da Informação (PPSI), obtido por cada órgão e entidade do Poder Executivo federal em 0,20 (dois décimos), até 2027.*

Análise das providências

16. *A IN SGD/MGI 4/2026 criou três indicadores de acompanhamento do PPSI 2.0: iBase, iSeg e iPriv:*

> *Art. 7º Ficam instituídos os seguintes indicadores:*
>
> *I - iBase: indicador usado para aferir a maturidade relacionada às medidas de estruturação básica para governança e de instrumentos fundamentais de privacidade e segurança da informação do órgão ou entidade;*
>
> *II - iSeg: indicador usado para aferir a maturidade relacionada às medidas de segurança da informação do órgão ou entidade; e*
>
> *III - iPriv: indicador usado para aferir a maturidade relacionada às medidas de privacidade do órgão ou entidade.*
>
> *§ 1º A aferição dos indicadores de maturidade iBase, iSeg e iPriv será realizada conforme disposto no Anexo IV.*
>
> *§ 2º O cálculo dos indicadores de que tratam os incisos I, II, e III do caput será realizado automaticamente pela ferramenta após o preenchimento dos níveis de implementação de todas as medidas do respectivo indicador.*

17. *Ademais, o iSeg tem meta explícita, fixada pela Portaria SGD/MGI 6.618/2024 (iniciativa 9.1 da EFGD) em incremento de 0,20 até 2027.*

18. *Ante o exposto, considera-se que medidas de controle foram adotadas para mitigar o risco.*

Risco RRA2 - Ausência, na estrutura de governança do PPSI, de atribuição explícita de responsabilidade para a AA das organizações quanto à implementação do PPSI

Providências adotadas pela SGD/MGI (peça 394, p. 2)

19. *A SGD/MGI afirma que incluiu previsão normativa para que a Alta Administração (AA) integre a estrutura de governança do PPSI.*

Análise das providências

20. *De acordo com o art. 7º, I, da Portaria 9.511/2025, a alta administração, nos termos do art. 2º, caput, inciso III, do Decreto nº 9.203, de 22 de novembro de 2017, compõe a estrutura de governança do PPSI. Já o art. 8º atribui à alta administração o fornecimento de recursos e a viabilização da estrutura de governança do PPSI.*

21. *Dessa forma, considera-se que medidas de controle foram adotadas para mitigar o risco de ausência de atribuição explícita de responsabilidade para a AA das organizações quanto à implementação do PPSI.*

Risco RRA3 - Escala de medição das medidas de segurança possibilita que acima de 50% seja considerado como implementado totalmente

Providências adotadas pela SGD/MGI (peça 394, p. 2)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

22. *SGD/MGI afirma que a escala foi revista e aprimorada.*

Análise das providências

23. *A versão 1.1.4 do guia do Framework (https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/arquivos-antigos/ppsi/guia_framework_psi.pdf) em seu capítulo 6, estabelecia que o nível de implementação 'Adota em maior parte ou totalmente' seria pontuado como 1 (nota máxima) se houvesse decisão formal ou plano aprovado e a medida na organização fosse implementada integralmente em mais de 50% ou em todos os ativos. Por meio da Instrução Normativa - 4/2026, o PPSI 2.0 passou a apresentar os seguintes níveis de implementação das medidas:*

> a) NÍVEIS DE IMPLEMENTAÇÃO DAS MEDIDAS AVALIADAS DE FORMA GRADUAL
>
> Tabela 3 - Níveis de implementação das medidas avaliadas de forma gradual e respectivas pontuações

Nível	Descrição	Pontuação
0 - Não se aplica	A medida não se aplica.	-
1 - Não adota ou há decisão formal	A medida é aplicável, mas não é implementada ou existe apenas um planejamento ou decisão formal para implementá-la.	0,00
2 - Inicial	A implementação da medida atende menos de 40% do seu propósito.	0,25
3 - Intermediário	A implementação da medida atende entre 40% e 80% do seu propósito.	0,50
4 - Completo	A implementação da medida atende mais de 80% do seu propósito.	0,75
5 - Aprimorado	A implementação da medida atende mais de 80% do seu propósito e é monitorada e revisada continuamente de forma sistemática, com base em métricas quantitativas, possuindo mecanismos que garantem uma implementação consistente ao longo do tempo.	1,00

24. *Ou seja, o nível 'Aprimorado' no PPSI 2.0 significa que a implementação da medida atende a mais de 80% de seu propósito e é monitorada e revisada sistematicamente.*

25. *Ante o exposto, considera-se que medidas de controle foram adotadas para mitigar o risco.*

Risco RPE1 - SGD/MGI apresenta limitação quantitativa em pessoal para as atividades do ciclo externo

Providências adotadas pela SGD/MGI

26. *A SGD/MGI informou que, no exercício de suas competências como órgão central do Sisp, também enfrenta limitação de pessoal para as atividades do ciclo externo (composto por etapas executadas pela SGD/MGI como acompanhamento e apoio), situação semelhante à dos demais órgãos do sistema (peça 394, p. 2). Como medida de reforço, foram realizados processos seletivos simplificados para a concessão de Gratificações do Sistema de Administração dos Recursos de Tecnologia da Informação (GSISP), contemplando níveis superior e intermediário, com foco nas áreas de privacidade e segurança da informação (peça 394, p. 2). Os servidores selecionados foram alocados na DEPSI/SGD, contribuindo para ampliar a capacidade operacional da unidade, ainda que de forma complementar às necessidades existentes (peça 394, p. 2).*

27. *Na fase de 'Comentários do gestor', a SGD/MGI informou que (peça 441, p. 2):*

> *No último concurso para a carreira de Analista em Tecnologia da Informação - ATI, foram nomeados 182 servidores em 2025 e 235 em 2026, dos quais 170 e 221, respectivamente, entraram em exercício. Apesar dos novos ingressos, o quantitativo foi inferior ao esperado, além das vacâncias ocorridas no período.*
>
> *Solicitou a realização de novo concurso público para o provimento de 494 vagas, conforme Nota Técnica SEI nº 17861/2026/MGI (Processo SEI*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

nº 19974.000518/2026-10). Também foi proposta a ampliação da carreira de 1.300 para 3.000 cargos, conforme Nota Técnica SEI nº 35837/2026/MGI (Processo SEI nº 19974.001171/2026-14).

Análise das providências

28. *Verifica-se que medidas de controle foram adotadas: a SGD/MGI apresentou três editais por meio dos quais tornou pública a realização de processo seletivo simplificado para a distribuição de GSISP para as áreas de privacidade e segurança da informação, destinadas à atuação junto aos Institutos Federais de Educação, Ciência e Tecnologia e Universidades Federais integrantes do Sisp. Da mesma forma, apresentou 24 portarias de pessoal por meio das quais concedeu-se a GSISP aos servidores selecionados. No mesmo sentido, houve a nomeação de Analistas em Tecnologia da Informação em 2025 e 2026.*

29. *Contudo, a própria Secretaria reconhece que o incremento de pessoal foi insuficiente para suprir a demanda, em razão de o quantitativo de nomeações ter ficado abaixo do esperado e da ocorrência de vacâncias no período. A dependência de novos concursos e da ampliação da estrutura da carreira de ATI evidencia que a limitação de pessoal é um desafio de natureza estrutural, que transcende a governabilidade imediata da Secretaria.*

30. *Nesse contexto, embora as providências adotadas demonstrem o empenho da Secretaria em tratar a deficiência de recursos humanos, o risco RPE1 permanece presente. A medida é considerada em implementação, uma vez que a efetiva mitigação do risco depende de fatores externos, como a autorização de novos certames e a expansão do quadro de pessoal, elementos que ainda não foram plenamente concretizados.*

31. *Portanto, conclui-se que o risco RPE1 subsiste.*

Risco RPE2 - Organizações do Sisp têm deficiências em pessoal (quantidade e/ou qualificação) para as atividades do ciclo interno

Providências adotadas pela SGD/MGI (peça 394, p. 3)

32. *A SGD/MGI informou que, no exercício de suas competências como órgão central do Sisp e supervisor da carreira de ATI, identifica que o risco é relevante, com evidências de insuficiência de pessoal, principalmente em termos quantitativos, afetando a execução das atividades do ciclo interno (composto por etapas a serem executadas pelo órgão implementador do framework).*

33. *De acordo com a Secretaria, as análises técnicas já realizadas mostram um déficit estrutural de profissionais de TI. Isso se reflete em dificuldades nas atividades de governança, desenvolvimento, segurança da informação e gestão de contratações, além de equipes reduzidas, sobrecarga de trabalho e atrasos em projetos, comprometendo a execução de funções essenciais.*

34. *Registrou-se, ainda, que, embora tenha havido a nomeação de 181 ATIs em setembro de 2025, o quantitativo de pessoal permanece aquém do necessário para atender às demandas dos órgãos do Sisp. Nesse contexto, a Secretaria formalizou a solicitação de provimento de 494 vagas de ATI e encaminhou ofício à Secretaria de Gestão de Pessoas do MGI (SGP/MGI), destacando os desafios relacionados à atratividade da carreira, especialmente a defasagem remuneratória em relação a outras carreiras e ao setor privado, com impacto na atração e retenção de profissionais, na evasão e na recomposição da força de trabalho.*

35. *Adicionalmente, informou que a Portaria - SGD/MGI 1.010/2026 redistribuiu as GSISP, com foco também nas áreas de segurança da informação e privacidade. Segundo o órgão, a medida contribui para reforçar essas frentes, mas não resolve a necessidade estrutural de pessoal diante das demandas do Sisp.*

36. *Quanto à qualificação, a SGD/MGI afirmou que vem mantendo ações contínuas de*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

capacitação no Sisp. Um exemplo é o MBA em Privacidade e Segurança da Informação, já na quinta turma, realizado em parceria com a Universidade de Brasília, com cerca de trinta vagas por turma e aberto a servidores de todos os órgãos. O curso busca preparar melhor os profissionais para atuar nessas áreas e apoiar o aumento da maturidade e da segurança nos órgãos.

Análise das providências

37. *A SGD/MGI reconhece a relevância do risco RPE2 e tem adotado medidas para mitigar a escassez de pessoal nas organizações do Sisp, destacando-se a redistribuição de gratificações (GSISP) com foco em segurança da informação e a promoção de ações de capacitação, como o MBA em parceria com a UnB. Além disso, a Secretaria tem atuado institucionalmente junto à SGP/MGI para pleitear o provimento de novas vagas e a revisão da atratividade da carreira de Analista em Tecnologia da Informação (ATI).*

38. *Não obstante o empenho da Secretaria, o déficit de profissionais de TI nas organizações do Sisp permanece como um desafio estrutural. A insuficiência quantitativa e a dificuldade de retenção de talentos, agravadas pela defasagem remuneratória em relação ao setor privado, comprometem a execução de funções essenciais de governança e segurança da informação, conforme relatado pela própria SGD/MGI.*

39. *Nesse contexto, a providência é considerada em implementação. Embora as ações de capacitação e os pleitos de recomposição da força de trabalho sejam passos necessários, a mitigação efetiva do risco depende de decisões que transcendem a governabilidade da SGD/MGI. Portanto, o risco RPE2 subsiste.*

Risco RPE3 - Em algumas organizações, existe uma rotatividade grande de pessoas no quadro

Providências adotadas pela SGD/MGI

40. *A SGD/MGI informou que, no exercício de suas competências como órgão central do Sisp e supervisor da carreira de Analista em Tecnologia da Informação (ATI), avalia que o risco é relevante, especialmente quanto à rotatividade de profissionais de TI. Ademais, as análises realizadas pela Secretaria mostram elevada rotatividade na carreira de ATI, com vacâncias, desistências e saídas para outros cargos. Esse cenário está ligado, principalmente, aos desafios de atratividade da carreira, em especial à defasagem remuneratória em relação a outras carreiras públicas e ao setor privado (peça 394, p. 3).*

41. *Segundo a SGD/MGI, a situação já foi registrada em Nota Técnica e em ofício encaminhado à SGP/MGI, que apontam a evasão e a dificuldade de recomposição da força de trabalho, indicando a necessidade de medidas estruturantes para reduzir o problema. Adicionalmente, a Portaria - SGD/MGI 1.010/2026, promoveu a redistribuição das GSISP, voltadas a servidores que atuam em TI, como forma de reforçar as equipes. Ainda assim, a medida não resolve o problema de rotatividade (peça 394, p. 3).*

42. *Na fase de 'Comentários do gestor', a SGD/MGI informou que (peça 441, p. 2-3):*

> *A carreira de ATI ainda apresenta dificuldades de retenção. As vacâncias reduzem a força de trabalho disponível e podem gerar perda de conhecimento e impactos na continuidade das atividades, projetos e serviços de tecnologia da informação. Essa situação está registrada na Nota Técnica SEI nº 35837/2026/MGI (Processo SEI nº 19974.001171/2026-14);*
>
> *Sobre a atratividade da carreira, a SGD já encaminhou à Secretaria de Gestão de Pessoas - SGP/MGI estudos que apontam a defasagem remuneratória e seus impactos na retenção dos ATIs, entre eles a Nota Técnica SEI nº 2442/2023/MGI e o Ofício SEI nº 44390/2026/MGI (Processo SEI nº 19974.000493/2026-46);*
>
> *No Ofício, a SGD solicitou à SGP/MGI a avaliação de medidas para melhorar a*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

atratividade da carreira, especialmente quanto à estrutura remuneratória. Mais recentemente, o Acórdão nº 1.475/2026-TCU-Plenário recomendou ao MGI, por intermédio da SGP, a implementação de ações concretas para superar os desafios relacionados à falta de atratividade da carreira de ATI, considerando, entre outros aspectos, a assimetria remuneratória em relação a carreiras equivalentes e ao mercado privado.

Análise das providências

43. *A SGD/MGI reconhece a relevância do risco de rotatividade na carreira de Analista em Tecnologia da Informação (ATI) e tem adotado medidas para mitigar seus impactos, como a redistribuição de gratificações (GSISP) e o encaminhamento de estudos técnicos à Secretaria de Gestão de Pessoas (SGP/MGI) visando à melhoria da atratividade da carreira.*

44. *Ressalte-se que a persistência desse risco é corroborada pelo Acórdão 1.475/2026-TCU-Plenário, relator Ministro Odair Cunha, que recomendou ao MGI a implementar ações concretas para superar a falta de atratividade da carreira de ATI. Enquanto não forem adotadas medidas estruturantes que garantam a retenção desses profissionais, a implementação do PPSI continuará vulnerável à descontinuidade técnica.*

45. *Portanto, a providência é considerada em implementação. O risco RPE3 subsiste, uma vez que as ações de mitigação adotadas pela SGD/MGI, embora pertinentes, não têm sido suficientes para reverter o quadro de evasão.*

Risco RPE4 - Ausência de designação do gestor de segurança da informação em 21% das organizações

Providências adotadas pela SGD/MGI

46. *A SGD/MGI informou que, no SisPPSI, ferramenta para preenchimento de informações relativas ao ciclo de implementação do framework PPSI, 232 órgãos informaram que designaram o gestor de segurança da informação, o que corresponde a 93% dos órgãos (peça 394, p. 3).*

47. *Esse número foi obtido verificando-se no banco de dados do SisPPSI, em 30/4/2026, o quantitativo de órgãos que possuíam registro dos dados do gestor de segurança da informação, independentemente de o órgão ter realizado ou não o envio da entrega de março/2026 (Ciclo 1 do PPSI 2.0). Considerando apenas os órgãos que realizaram o envio da entrega de março/2026 (Ciclo 1 do PPSI 2.0), são 224 organizações com gestor designado (peça 441, p, 3).*

Análise das providências

48. *Os dados brutos da peça 419 mostram 224 organizações com gestor designado e 15 sem designação, num universo de 239 respondentes (93,7%). Considerando os dados da peça 419, restam 15 organizações (6% do total) ainda sem gestor designado, o que representa uma melhora expressiva frente aos 21% do achado original.*

49. *Não obstante a melhoria, 15 organizações permanecem sem a devida designação, em desacordo com o art. 10, inciso III, do Decreto12.572/2025 e com o art. 18 da Instrução Normativa - GSI/PR 1/2020. A ausência dessa figura central na estrutura organizacional fragiliza a governança de segurança da informação, podendo resultar em ações descoordenadas, controles inconsistentes e maior exposição a incidentes cibernéticos.*

50. *É importante ressaltar que a adoção das medidas de controle relativas à designação do gestor de SI não está sob a governabilidade da SGD/MGI, cabendo a implementação dessas medidas pelas próprias organizações do Sisp.*

51. *No entanto, embora mitigado, o risco continua a existir, uma vez que quinze organizações do Sisp ainda não possuem gestor de SI designado, em desacordo com o Decreto 12.572/2025 e com a*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

Instrução Normativa GSI/PR 1/2020.

52. *Este risco é da responsabilidade das quinze organizações do Sisp. Mais ainda, constitui-se agora em desconformidade com normas em vigor, sendo passível de apuração de responsabilidade futura.*

Risco RPE5 - A Comissão de Coordenação do Sisp não participa da seleção dos controles priorizados em cada ciclo

Providências adotadas pela SGD/MGI

53. *A SGD/MGI afirma que os dados enviados pelas organizações do Sisp são críticos e não podem ser compartilhados com a Comissão. Ademais, destaca o contínuo alinhamento e envolvimento dos órgãos e entidades do Sisp quanto à evolução do PPSI, como, por exemplo, por meio de apresentações e Webinários (peça 394, p. 4).*

54. *Na fase de 'Comentários do gestor', a SGD/MGI informou que (peça 441, p. 3-4):*

> *Conforme informado na Nota Técnica SEI nº 18707/2026/MGI (SEI 60841079), a priorização de medidas no âmbito do PPSI é realizada pela SGD, adotando como principal critério a conformidade aos normativos vigentes, mais especificamente aos do Gabinete de Segurança Institucional da Presidência da República - GSI/PR e da Agência Nacional de Proteção de Dados - ANPD.*
>
> *Por essa razão, na Instrução Normativa SGD/MGI nº 4/2026 foi estabelecida a priorização de medidas específicas para o ciclo de 2026, permitindo direcionar esforços institucionais para temas considerados mais relevantes à evolução da maturidade em privacidade e segurança da informação; sem prejuízo dessa priorização, o normativo estabelece também as medidas de gestão contínua, que permanecem sujeitas a acompanhamento permanente. Esse modelo, que será mantido nos próximos ciclos do PPSI, busca equilibrar a orientação estratégica centralizada com a preservação de um núcleo estável e contínuo de governança, gestão de riscos e conformidade no âmbito do PPSI.*

Análise das providências

55. *O Decreto 7.579/2011, em seus arts. 4º e 5º, estabelece que a elaboração e a implementação de políticas e diretrizes do Sisp devem contar com a participação da Comissão de Coordenação. A SGD/MGI, ao centralizar a definição dos controles priorizados, tem restringido a atuação da Comissão a um papel meramente consultivo ou informativo, o que destoa da competência deliberativa ou participativa prevista no normativo.*

56. *O argumento da Secretaria de que os dados das organizações são sigilosos não justifica a exclusão da Comissão do processo decisório. Mesmo que a restrição a dados individualizados se justifique, isso não impede, em princípio, que a Comissão participe da definição da metodologia e dos critérios de priorização dos controles, algo que não exige acesso a dados de organizações específicas.*

57. *A realização de apresentações e webinários constitui medida de transparência, mas não supre a exigência legal de participação da Comissão na elaboração das diretrizes do Sisp. A ausência de um processo decisório participativo pode resultar em uma priorização de controles desconectada da realidade operacional das organizações, comprometendo a aderência e a eficácia do PPSI.*

58. *Portanto, o risco RPE5 permanece presente, uma vez que a SGD/MGI mantém a centralização da tomada de decisão, em descompasso com o modelo de governança colaborativa estabelecido pelo Decreto 7.579/2011.*

Risco RIN1 - ausência de informações (evidências) sobre a implementação dos controles, pois o PPSI é implementado por meio de autoavaliação

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

Providências adotadas pela SGD/MGI (peça 394, p. 4)

59. *De acordo com a SGD/MGI, as evidências acerca da implementação das medidas podem ser informadas pelos órgãos diretamente no SisPPSI.*

60. *Na fase de 'Comentários do gestor', a SGD/MGI informou que (peça 441, p. 4):*

> *A Portaria SGD/MGI nº 9.511, de 2025 admite, em seu art. 17, registro de evidências da implementação das medidas – de forma facultativa. Tal iniciativa vai ao encontro do aprimoramento da maturidade do PPSI, por meio da realização de mudanças gradativas no Programa para todos os órgãos do SISP, considerando inclusive o esforço futuro da SGD quanto à análise das evidências que passarem a ser compulsórias nos ciclos vindouros do PPSI;*
>
> *Nesse sentido, como medida mitigatória, serão consignadas, na instrução normativa que regerá o Ciclo 2027 do PPSI 2.0, quais medidas deverão necessariamente ter o registro das evidências, na hipótese de o órgão consigná-la como implementadas.*

Análise das providências

61. *O art. 17 da Portaria - SGD/MGI 9.511/2025 estabelece que a Secretaria de Governo Digital pode solicitar evidências da implementação das medidas de privacidade e segurança da informação para fins de análise, monitoramento e adequação do apoio ao PPSI.*

62. *Embora a referida norma preveja a possibilidade de registro de evidências, a natureza facultativa dessa medida não é suficiente para mitigar o risco de que as organizações reportem níveis de maturidade superiores à realidade, gerando uma falsa sensação de segurança. Ademais, embora a previsão de tornar compulsório o registro de evidências para medidas selecionadas no Ciclo 2027 represente um avanço, a fidedignidade das informações ainda permanece vinculada à autodeclaração dos gestores, sem a obrigatoriedade de comprovação documental.*

63. *Dessa forma, o risco de falsa sensação de segurança, que leva a organização a acreditar que está mais protegida do que realmente está, permanece presente, a despeito das medidas de controle adotadas pela SGD/MGI e do planejamento para a exigência de evidências a partir de 2027.*

Risco RPR2 - Ausência de agrupamento das organizações por tamanho, finalidade, similaridade ou outro critério possível

Providências adotadas pela SGD/MGI (peça 394, p. 4)

64. *De acordo com a SGD/MGI, estão previstos estudos, a serem concluídos em 2027, para categorização e/ou agrupamento dos órgãos, para além do agrupamento por finalidade já utilizado na atualidade (Agência, Fundação, Instituto Federal, Ministério, Superintendência, Universidade, Outros). Uma das referências para o desenvolvimento desses estudos será o modelo de maturidade institucional em cibersegurança, em elaboração pelo Grupo de Trabalho Temático (GTT), instituído pelo Comitê Nacional de Cibersegurança (CNCiber). O GTT é coordenado pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).*

65. *O modelo institucional proposto buscará integração com o PPSI, conforme previsto no item 1.12 da ata da 9ª reunião ordinária do CNCiber. A conclusão dos trabalhos do GTT está prevista para julho de 2026, a ser submetida a instâncias superiores de aprovação.*

66. *Na fase de 'Comentários do gestor', a SGD/MGI informou que (peça 441, p. 4):*

> *A ausência de classificação geral dos órgãos por porte ou outro critério não implica tratamento inteiramente uniforme. No exercício de suas competências de orientação, apoio e acompanhamento dos órgãos e entidades do SISP, a SGD adota estratégias diferenciadas segundo características e necessidades comuns;*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

> *Nesse contexto, esta Secretaria mantém um grupo destinado ao apoio, monitoramento e acompanhamento do PPSI nas instituições federais de ensino, consideradas suas características institucionais comuns (conforme item 5.2, 4ª linha da tabela da Nota Técnica 18707 (SEI 60841079). Também informa ao Esplanada +Segura, fórum que reúne ministérios para o tratamento coordenado de temas compartilhados no Poder Executivo federal, os aspectos relativos às temáticas de privacidade, segurança da informação e combate a fraudes digitais determinados no âmbito do PPSI - tendo, inclusive, participado da 19ª Reunião do Fórum de Secretários-Executivos em 3/9/2026, para apresentação de informações sobre o PPSI;*
>
> *Tais iniciativas constituem formas de agrupamento por finalidade e similaridade, permitindo orientação mais aderente às necessidades dos respectivos conjuntos de organizações, sem prejuízo de eventual adição futura de critérios adicionais de segmentação.*

Análise das providências

67. *A ausência de agrupamento das organizações por tamanho, finalidade, similaridade ou outro critério possível pode levar a comparações insuficientes entre as organizações, com a seguinte consequência: organizações desestimuladas a continuar com a implementação do framework, o que leva a ineficácia em cumprir o objetivo do programa.*

68. *Ressalta-se que a adoção de estratégias pontuais e diferenciadas na orientação, apoio e acompanhamento pela SGD/MGI é relevante e constitui boa prática, mas não supre a carência de uma metodologia de governança que preveja metas, prazos e níveis de maturidade diferenciados por segmento.*

69. *Portanto, embora os estudos iniciados pela Secretaria para a categorização dos órgãos representem um avanço, o risco RPR2 permanece presente, uma vez que a estrutura atual do PPSI ainda não incorpora critérios de segmentação formalizados.*

Risco RPR3 - Ausência de mecanismo de cumprimento (enforcement) na implementação do framework pelas organizações do Sisp

Providências adotadas pela SGD/MGI

70. *A SGD/MGI informou que incluiu previsão normativa acerca do enforcement para que os órgãos e entidades do Sisp implementem o PPSI (peça 394, p. 4).*

71. *No entanto, afirma que não dispõe de competência legal para aplicar sanções orçamentárias, funcionais ou de desempenho às altas administrações dos demais órgãos (peça 441, p. 5). Entende, ainda, que o fluxo de tratamento deve combinar:*

71.1. obrigação normativa (contemplada, na atualidade, por meio da Portaria - SGD/MGI 9.511, de 2025, e da Instrução Normativa - SGD/MGI 4, de 2026);

71.2. registro de inadimplência (consignada por meio da ferramenta SisPPSI);

71.3. comunicações formais (ofícios encaminhados aos órgãos Sisp);

71.4. ciência às altas administrações (apresentada entre outros, no Esplanada +Segura);

71.5. atuação dos controles internos (responsável setorial pela gestão da integridade integrando a estrutura de governança do PPSI);

71.6. ciência aos órgãos de controle, quando cabível.

72. *A Secretaria entende, ainda, que o controle externo constitui elemento relevante de enforcement (peça 441, p. 5).*

Análise das providências

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

73. *Estabelecer a obrigatoriedade em portaria é apenas o primeiro passo; o enforcement pressupõe a existência de consequências concretas para o descumprimento, tais como a vinculação a metas de desempenho da alta administração, o condicionamento de recursos orçamentários ou a exposição pública da inadimplência em relatórios de gestão.*

74. *Embora a Secretaria liste uma série de ações de monitoramento (registro de inadimplência, ofícios, fóruns e ciência aos órgãos de controle), tais medidas possuem caráter predominantemente informativo e não garantem, por si sós, a mudança de comportamento dos gestores inadimplentes. A ausência de um mecanismo que torne o descumprimento do PPSI um fator de risco para a gestão do órgão esvazia a força coercitiva da norma.*

75. *É compreensível a limitação da SGD/MGI quanto à aplicação de sanções diretas, dada a sua natureza de órgão central. Contudo, enquanto não houver um mecanismo que vincule o cumprimento do programa a consequências administrativas ou de desempenho, a implementação do PPSI continuará dependente da voluntariedade dos gestores.*

76. *Portanto, conclui-se que o risco RPR3 permanece presente, uma vez que as medidas adotadas até o momento não foram suficientes para conferir a necessária efetividade ao cumprimento das diretrizes do programa.*

77. *Registre-se que, se a SGD/MGI como órgão central do Sisp entende que não tem competência suficiente para o enforcement, ainda que a combinação de normativos utilizada nesta análise permita depreender tal competência, ela pode tratar o risco propondo normatização mais clara e de mais alto nível, como, por exemplo, estabelecer o programa por normativo hierarquicamente superior (como um Decreto) e regulamentá-lo por portaria, como vem fazendo.*

Risco RPR4 - Não há uma forma de pré-preenchimento com as respostas do ciclo anterior c/c mudança do modelo do instrumento a cada ciclo

Risco RTE1 - Ferramenta de acompanhamento da implementação do framework no formato de planilha eletrônica. Nem todas as organizações do Sisp possuem o Microsoft Excel para preencher o diagnóstico e o plano de trabalho

Providências adotadas pela SGD/MGI (peça 394, p. 4)

78. *A SGD/MGI informou que foi desenvolvida e implantada ferramenta para preenchimento, pelos órgãos, das informações sobre o diagnóstico e o plano de trabalho.*

Análise das providências

79. *Conforme a seção 'Ferramentas do Framework do PPSI' no site do MGI, o preenchimento do nível de implementação das medidas do framework do PPSI até o ciclo 5 era realizado por meio de ferramenta no formato .xlsx e os dados eram consolidados no Painel de Business Intelligence (BI). No entanto, de acordo com o art. 5º da IN, a SGD/MGI disponibilizaria ferramenta para preenchimento de informações relativas ao ciclo de implementação de 2026 do framework do PPSI. Ademais, conforme o art. 6º, o diagnóstico e o plano de trabalho resultante da etapa de planejamento do PPSI deveriam ser encaminhados à SGD/MGI, exclusivamente por meio da ferramenta de que trata o art. 5º, até 27 de fevereiro de 2026.*

80. *A ferramenta de que trata a IN é o SisPPSI, que foi desenvolvida para a realização da autoavaliação. Dessa forma, considera-se que os riscos foram mitigados.*

Risco RPR5 - Gestores das organizações desconhecem o modelo de três linhas de defesa, acreditando que o setor de SegCiber da organização é o único responsável pela gestão de riscos de SegCiber

Providências adotadas pela SGD/MGI (peça 394, p. 5)

81. *A SGD/MGI informou que incluiu previsão normativa acerca da competência para gestão*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

de riscos relacionados à segurança da informação e privacidade.

Análise das providências

82. *A Portaria - SGD/MGI 9.511/2025 traz dispositivos no sentido de que compete à alta administração gerir os riscos no âmbito organizacional. Em adição, o Guia do Framework de Privacidade e Segurança da Informação versão 1.2 estabelece que o controle 'Estruturação básica para governança' inclui os papéis essenciais para a condução da governança em privacidade e segurança da informação, tais como a alta administração, o gestor de segurança da informação, o encarregado pelo tratamento de dados pessoais, o gestor de Tecnologia da Informação e Comunicação (TIC) e o responsável pela gestão da integridade. Ademais, estabelece que esses papéis são decisivos para o alinhamento estratégico, operacional e de responsabilização, garantindo o cumprimento das diretrizes e a efetividade das ações propostas no framework.*

83. *A medida de controle 0.1 é a seguinte: 'A alta administração do órgão estabelece, mantém, monitora e aprimora o sistema de gestão de riscos e controles internos relativos aos temas de privacidade e segurança da informação?'. A descrição dessa medida estabelece que, conforme Acórdão 2.387/2024-TCU-Plenário, a alta administração da organização deve liderar o processo de gestão de riscos decorrentes de ataques cibernético.*

84. *Dessa forma, considera-se que o risco foi mitigado.*

Risco RRE1 - Insuficiência de recursos financeiros para implementação das medidas priorizadas nas organizações do Sisp

Providências adotadas pela SGD/MGI (peça 394, p. 5)

85. *A SGD/MGI informou que foi incluída previsão normativa acerca da competência da alta administração dos órgãos e entidades do Sisp para fornecer os recursos necessários para assegurar a gestão da privacidade e da segurança da informação, de modo a adotar decisões sobre privacidade e segurança da informação em um nível de relevância e prioridade adequadas e alinhadas com a estratégia e com a consecução dos objetivos do órgão ou entidade no cumprimento da sua missão institucional.*

Análise das providências

86. *O art. 8º da Portaria 9.511/2025 atribui à Alta Administração dos órgãos do Sisp a competência de fornecer os recursos necessários à gestão de privacidade e segurança da informação, em nível compatível com a estratégia e os objetivos da instituição.*

87. *Entretanto, estabelecer uma competência em norma não é o mesmo que garantir seu cumprimento. E, no caso de recursos financeiros, a limitação pode não ser só falta de prioridade institucional, pode ser falta real de orçamento disponível, por contingenciamento ou teto de gastos. Nesse segundo caso, nenhum mecanismo de enforcement resolveria o problema sozinho.*

88. *Dessa forma, considera-se que a SGD/MGI adotou medidas de controle, mas o risco RRE1 permanece presente.*

Conclusão

89. *Após a análise das respostas da SGD para os riscos identificados pela equipe de auditoria, têm-se que:*

89.1. as medidas de controle adotadas foram suficientes para mitigar os seguintes riscos:

89.1.1. Risco RRA1 - Insuficiência de indicadores e metas do programa;

89.1.2. Risco RRA2 - Ausência, na estrutura de governança do PPSI, de atribuição explícita de responsabilidade para a AA das organizações quanto à implementação do PPSI;

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

89.1.3. Risco RRA3 - Escala de medição das medidas de segurança possibilita que acima de 50% seja considerado como implementado totalmente;

89.1.4. Risco RPR4 - Não há uma forma de pré-preenchimento com as respostas do ciclo anterior c/c mudança do modelo do instrumento a cada ciclo;

89.1.5. Risco RPR5 - Gestores das organizações desconhecem o modelo de três linhas de defesa, acreditando que o setor de SegCiber da organização é o único responsável pela gestão de riscos de SegCiber;

89.1.6. Risco RTE1 - Ferramenta de acompanhamento da implementação do framework no formato de planilha eletrônica. Nem todas as organizações do Sisp possuem o Microsoft Excel para preencher o diagnóstico e o plano de trabalho.

89.2. os seguintes riscos continuam presentes:

89.2.1. Risco RPE1 - SGD/MGI apresenta limitação quantitativa em pessoal para as atividades do ciclo externo;

89.2.2. Risco RPE2 - Organizações do Sisp têm deficiências em pessoal (quantidade e/ou qualificação) para as atividades do ciclo interno;

89.2.3. Risco RPE3 - Em algumas organizações, existe uma rotatividade grande de pessoas no quadro;

89.2.4. Risco RPE4 - Ausência de designação do gestor de segurança da informação em 21% das organizações;

89.2.5. Risco RPE5 - A Comissão de Coordenação do Sisp não participa da seleção dos controles priorizados em cada ciclo;

89.2.6. Risco RIN1 - Ausência de informações (evidências) sobre a implementação dos controles, pois o PPSI é implementado por meio de autoavaliação;

89.2.7. Risco RPR2 - Ausência de agrupamento das organizações por tamanho, finalidade, similaridade ou outro critério possível;

89.2.8. Risco RPR3 - Ausência de mecanismo de cumprimento (enforcement) na implementação do framework pelas organizações do Sisp;

89.2.9. Risco RRE1 - Insuficiência de recursos financeiros para implementação das medidas priorizadas nas organizações do Sisp.

90. *Com respeito a escassez de pessoal de TI no Sisp, o TCU já se manifesta sobre o tema desde 2014 (Acórdão 1.200/2014-TCU-Plenário, Relator Ministro Raimundo Carreiro). As medidas de restruturação das carreiras e gratificações não têm se mostrado eficazes para solucionar o problema da falta de pessoal, que se agrava na área de segurança da informação ante alta complexidade da área, o que exige profissionais altamente qualificados.*

91. *Nesse sentido, cabe registrar o contido no Acórdão 1.475/2026-TCU-Plenário, Rel. Ministro Odair Cunha:*

> *1.7.1. recomendar ao Ministério da Gestão e da Inovação em Serviços Públicos, por intermédio da Secretaria de Gestão de Pessoas, em articulação com a Secretaria de Governo Digital, que implemente ações concretas e eficazes que visem superar os desafios relacionados à falta de atratividade da carreira de Analista em Tecnologia da Informação, levando em consideração, entre outros aspectos, a assimetria remuneratória existente entre os ocupantes dessa carreira e profissionais equivalentes da Administração Pública e do mercado privado, com vistas a possibilitar o aumento da retenção de profissionais qualificados e da ocupação dos cargos disponíveis, de*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

> *forma a contribuir para o fortalecimento da área de tecnologia da informação no setor público e para a melhoria da qualidade, da segurança e da continuidade dos serviços digitais prestados à sociedade.*

92. *Ante todo o exposto, será proposto considerar parcialmente implementada a recomendação 9.1 do Acórdão 2.387/2024-TCU-Plenário, de relatoria do Ministro Augusto Nardes.*

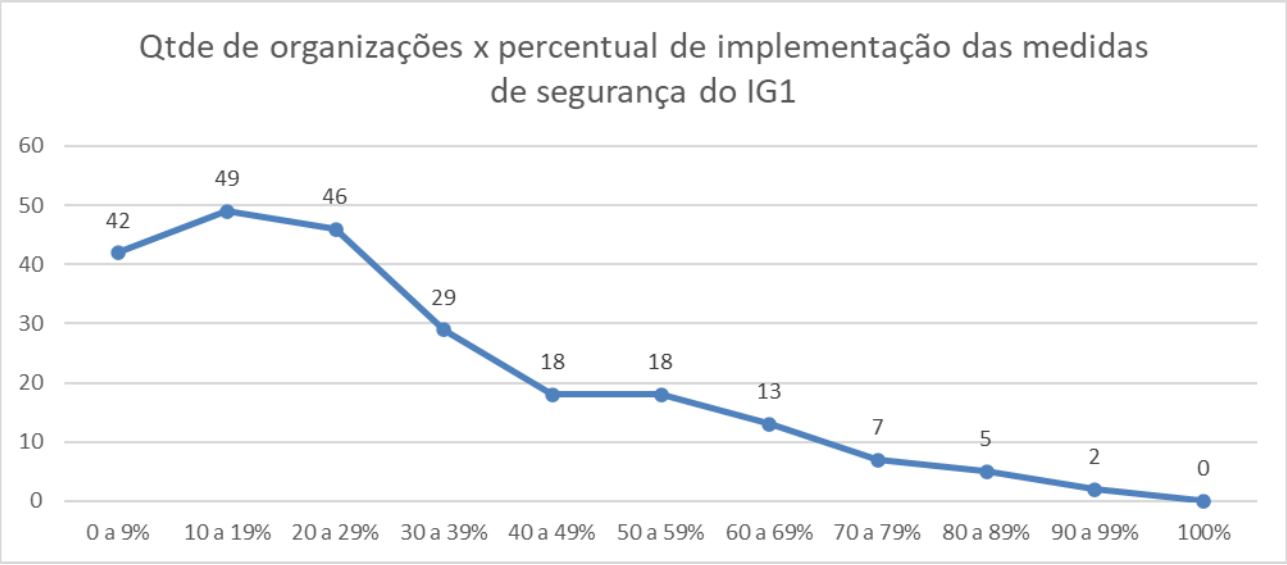
Recomendação 9.2.1

> *9.2. recomendar a cada uma das organizações do Sisp relacionadas no apêndice E do relatório de peça 200 que:*
>
> *9.2.1. adotem medidas para implementar os controles de segurança cibernética necessários para reduzir o risco de ataques cibernéticos ao nível aceitável para as políticas públicas que executam, utilizando como referencial as diretrizes expedidas pela SGD/MGI por meio do PPSI, de acordo com o art. 8º da Portaria-SGD/MGI nº 852/2023;*

Situação que levou à proposição da deliberação

93. *Com base nos questionários de 229 diferentes organizações do Sisp que responderam ao ciclo 1 ou 2 do PPSI 1.0, a equipe de auditoria identificou que nenhuma das 229 organizações respondentes implementava as 56 medidas de segurança do IG1; apenas duas organizações implementam mais de 90% dessas medidas; e apenas 14 implementam mais de 70% (peça 3, p. 12).*

Figura 1: Percentual de implementação das medidas do IG1



Fonte: Equipe de auditoria

94. *Como consequência desse cenário, concluiu-se que as organizações do Sisp não estariam protegidas contra os ataques cibernéticos mais comuns, uma vez que o IG1 é definido como o conjunto básico de medidas de segurança de defesa cibernética que todas as organizações deveriam adotar para se protegerem contra esses ataques (peça 3, p. 15).*

Providências adotadas pelas organizações do Sisp

95. *Em resposta ao Ofício 11923/2026-TCU/Seproc, a SGD/MGI enviou tabela em formato digital com cópia dos dados coletados da implementação do Framework PPSI 2.0, de 2026, pelas organizações do Sisp, os 18 controles e as 153 medidas de segurança do Segmento de Segurança da Informação (peça 419). Na tabela, constam 252 diferentes organizações. No entanto, 13 dessas organizações não preencheram o autodiagnóstico de segurança da informação e privacidade prevista no PPSI, restando 239 com respostas completas.*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

96. *Conforme o guia do PPSI vigente à época da fiscalização (Versão 1.1.3, de março de 2024), na etapa de avaliação, cada organização deveria analisar cada uma das medidas de segurança, individualmente, aplicando um nível de implementação para cada uma delas, dentre as seguintes possíveis:*

96.1. A organização não adota essa medida – Pontuação 0;

96.2. Há decisão formal ou plano aprovado para implementar – Pontuação 0.25;

96.3. Adota parcialmente: a medida na organização é implementada parcialmente em mais de 50% dos ativos – Pontuação 0.5;

96.4. Adota em menor parte: a medida na organização é implementada integralmente em menos de 50% dos ativos – Pontuação 0.75;

96.5. Adota em maior parte ou totalmente: a medida na organização é implementada integralmente em mais de 50% ou em todos os ativos – Pontuação 1.

97. *Ou seja, mesmo que a medida fosse implementada apenas em 50,01% dos ativos, para fins da avaliação, era considerado que as organizações adotavam em maior parte ou totalmente.*

98. *Por meio da Instrução Normativa – SGD/MGI 4/2026, o PPSI 2.0 passou a apresentar os seguintes níveis de implementação das medidas:*

98.1. 0 – Não se aplica: a medida não se aplica;

98.2. 1 – Não adota ou há decisão formal: a medida é aplicável, mas não é implementada ou existe apenas um planejamento ou decisão formal para implementá-la: Pontuação 0;

98.3. 2 – Inicial: a implementação da medida atende menos de 40% do seu propósito: Pontuação 0.25;

98.4. 3 – Intermediário: a implementação da medida atende entre 40% e 80% do seu propósito: Pontuação 0.50;

98.5. 4 – Completo: a implementação da medida atende mais de 80% do seu propósito: Pontuação 0.75;

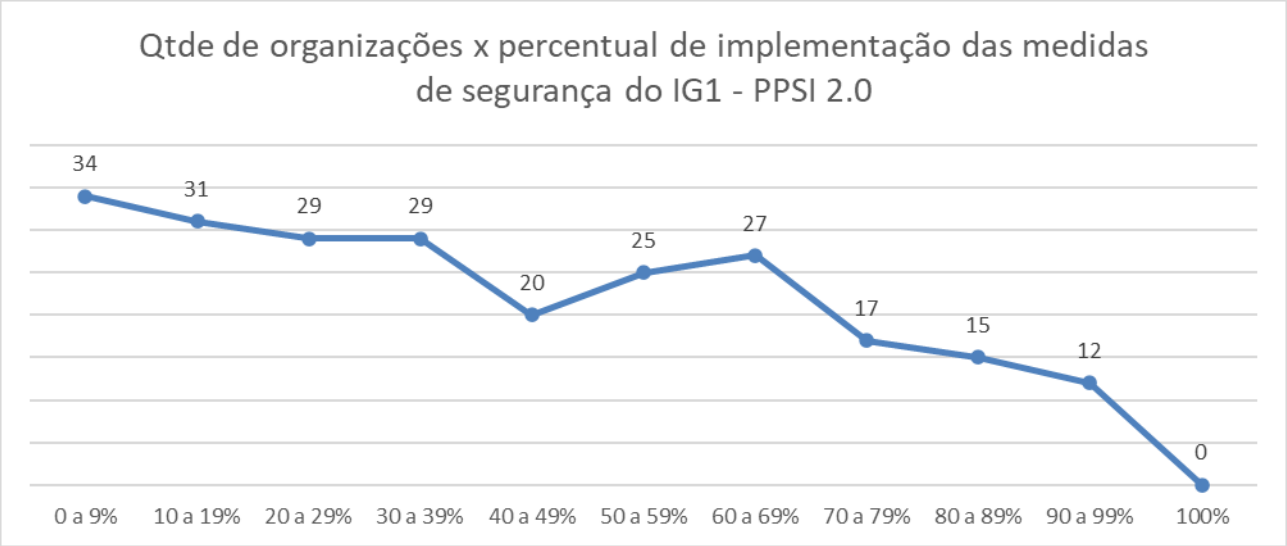
98.6. 5 – Aprimorado: a implementação da medida atende mais de 80% do seu propósito e é monitorada e revisada continuamente de forma sistemática, com base em métricas quantitativas, possuindo mecanismos que garantem uma implementação consistente ao longo do tempo: Pontuação 1.0.

99. *Para fins de comparação, considera-se, neste monitoramento, que a medida está implementada se apresentar os níveis Completo ou Aprimorado, o que significa que atende mais de 80% do seu propósito.*

100. *Dessa forma, com base na tabela enviada pela SGD/MGI contendo os dados coletados da implementação do Framework PPSI 2.0 por 239 organizações do SISP, verifica-se que a situação continua de alto risco: nenhuma organização atende ao grupo de implementação IG1 do guia Controles CIS versão 8.1. Ademais, verifica-se que doze organizações implementariam mais de 90% dessas medidas, enquanto 44 implementariam mais de 70%, o que significa um aumento comparado ao verificado em 2024 quando duas organizações implementariam mais de 90% dessas medidas e catorze implementariam mais de 70%.*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

Figura 3 - Número de organizações em cada faixa de implementação do IG1 no PPSI 2.0



Fonte: elaboração própria

101. *Em relação às 56 medidas de segurança do IG1, a tabela a seguir mostra o percentual de organizações que implementavam cada controle no mais alto nível de implementação: 'Adota em maior parte ou totalmente' e o percentual que implementaria atualmente cada medida nos níveis Completo ou Aprimorado:*

Tabela 1 - Percentual de organizações que implementam cada medida de segurança

Medida de segurança	*% de organizações que implementavam em maior parte ou totalmente – PPSI 1.0 Ciclos 1 e 2*	*% de organizações com níveis Completo ou Aprimorado – PPSI 2.0 Ciclo 2026*
1.1 O órgão estabelece e mantém um inventário detalhado de ativos institucionais?	*34%*	*43%*
1.2 O órgão trata ativos institucionais não autorizados?	*20%*	*32%*
2.1 O órgão estabelece e mantém um inventário de soluções de software?	*32%*	*42%*
2.2 O órgão mantém em seu ambiente computacional apenas soluções de software suportadas pelos seus fornecedores?	*25%*	*38%*
2.3 O órgão trata o uso de soluções de software não autorizadas?	*20%*	*32%*
3.1 O órgão estabelece e mantém um processo de gestão de dados?	*10%*	*15%*
3.2 O órgão estabelece e mantém um inventário de dados?	*13%*	*16%*
3.3 O órgão configura listas de controle de acesso a dados?	*40%*	*43%*
3.4 O órgão aplica retenção de dados?	*16%*	*22%*
3.5 O órgão descarta dados com segurança?	*10%*	*11%*
3.6 O órgão criptografa dados críticos em dispositivos de usuário final?	*8%*	*16%*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

4.1 O órgão estabelece e mantém um processo de configuração segura?	*22%*	*29%*
4.2 O órgão estabelece e mantém um processo de configuração segura para a infraestrutura de rede?	*34%*	*49%*
4.3 O órgão configura o bloqueio automático de sessão nos ativos institucionais?	*40%*	*60%*
4.4 O órgão implementa e gerencia um firewall nos servidores?	*67%*	*69%*
4.5 O órgão implementa e gerencia um firewall em dispositivos do usuário final?	*47%*	*54%*
4.6 O órgão gerencia com segurança os ativos institucionais e soluções de software?	*30%*	*47%*
4.7 O órgão gerencia contas padrão?	*63%*	*63%*
5.1 O órgão estabelece e mantém um inventário de contas?	*39%*	*57%*
5.2 O órgão promove ações para evitar a reutilização de senhas?	*20%*	*47%*
5.3 O órgão desabilita ou exclui contas inativas?	*39%*	*58%*
5.4 O órgão limita os privilégios de administrador às contas de administrador dedicadas?	*56%*	*62%*
6.1 O órgão estabelece um processo de concessão de acesso?	*51%*	*58%*
6.2 O órgão estabelece um processo de revogação de acesso?	*38%*	*49%*
6.3 O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para soluções de software expostas externamente?	*11%*	*29%*
6.4 O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para acesso remoto à rede?	*17%*	*42%*
6.5 O órgão exige autenticação multifator (Multi-Factor Authentication, MFA) para acesso administrativo?	*13%*	*36%*
7.1 O órgão estabelece e mantém um processo de gestão de vulnerabilidade?	*14%*	*27%*
7.2 O órgão estabelece e mantém um processo de remediação?	*8%*	*19%*
7.3 O órgão executa a gestão automatizada de atualizações do sistema operacional?	*33%*	*41%*
7.4 O órgão executa a gestão automatizada de atualizações de aplicações?	*17%*	*25%*
8.1 O órgão estabelece e mantém um processo de gestão de logs de auditoria?	*18%*	*26%*
8.2 O órgão coleta logs de auditoria?	*21%*	*32%*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

8.3 O órgão armazena adequadamente os logs de auditoria?	*24%*	*32%*
9.1 O órgão permite o uso apenas de navegadores e clientes de e-mail totalmente suportados por seus fornecedores?	*33%*	*46%*
9.2 O órgão usa serviços de filtragem de Sistema de Nomes de Domínio (Domain Name System, DNS?	*54%*	*60%*
10.1 O órgão instala e mantém um software antimalware?	*58%*	*66%*
10.2 O órgão configura atualizações automáticas de assinatura antimalware?	*58%*	*67%*
10.3 O órgão desabilita a execução e reprodução automática para mídias removíveis?	*27%*	*41%*
11.1 O órgão estabelece e mantém um processo de realização de cópias de segurança (backup)?	*31%*	*69%*
11.2 O órgão executa backups automatizados?	*76%*	*77%*
11.3 O órgão protege os dados de recuperação?	*40%*	*56%*
11.4 O órgão estabelece e mantém uma instância isolada de dados de recuperação?	*39%*	*50%*
12.1 O órgão mantém atualizada a infraestrutura de rede?	*31%*	*51%*
14.1 O órgão implementa um programa de conscientização em segurança da informação?	*17%*	*38%*
14.2 O órgão conscientiza os agentes públicos para reconhecer ataques de engenharia social?	*9%*	*36%*
14.3 O órgão conscientiza os agentes públicos nas melhores práticas de autenticação?	*14%*	*35%*
14.4 O órgão conscientiza os agentes públicos nas melhores práticas de tratamento de dados?	*6%*	*25%*
14.5 O órgão conscientiza os agentes públicos sobre as causas ocorrências não intencionais que podem expor dados?	*8%*	*25%*
14.6 O órgão conscientiza os agentes públicos sobre como reconhecer e notificar incidentes de segurança da informação?	*8%*	*26%*
14.7 O órgão conscientiza os agentes públicos sobre como identificar e comunicar se os ativos institucionais estão sem atualizações de segurança?	*5%*	*22%*
14.8 O órgão conscientiza os agentes públicos sobre os perigos de se conectar e	*8%*	*28%*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

transmitir dados organizacionais em redes inseguras?		
15.1 O órgão estabelece e mantém o inventário de provedores de serviços?	*27%*	*36%*
17.1 O órgão designou agente responsável, e respectivo substituo, para gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)?	*57%*	*75%*
17.2 O órgão estabelece e mantém informações de contato para notificar incidentes de segurança da informação?	*51%*	*59%*
17.3 O órgão estabelece e mantém um processo institucional para notificar incidentes de segurança da informação?	*32%*	*46%*

Análise das providências

102. *Antes de se proceder à análise da implementação da recomendação, fazem-se necessários dois esclarecimentos metodológicos.*

103. *O ministro relator, em seu relatório, ponderou que, quanto às recomendações destinadas às 254 organizações do Sisp, a unidade técnica deveria observar, além da conveniência e oportunidade, a forma mais eficiente de realizar seu monitoramento. Dada a elevada quantidade de organizações, foi facultada à AudTI a adoção de amostragem, o monitoramento no curso de outras ações de controle ou outra estratégia que se mostrasse mais eficiente do que a atuação em cada uma das 254 organizações (peça 8, p. 31).*

104. *Nesse sentido, em instrução anterior, consolidou-se o entendimento de que (peça 367, p. 3):*

104.1. A recomendação contida no item 9.2.1 é de caráter sistêmico, direcionada a todas as organizações do Sisp;

104.2. Compete à SGD/MGI, no âmbito do PPSI, 'diagnosticar o grau de implementação dos controles de privacidade e segurança da informação pelos órgãos e entidades pertencentes ao SISP' e 'acompanhar a implementação de controles e sensibilizar de forma contínua a Estrutura de Governança, prevista no art. 6º desta Portaria' (art. 4º, § 1º, incisos III e IV, respectivamente, da Portaria - SGD/MGI 852/2023);

104.3. O monitoramento, pelo TCU, do cumprimento da recomendação em cada organização do Sisp demandaria um esforço superior ao resultado pretendido;

104.4. A existência de um programa em andamento como o PPSI permite uma atuação eficiente e centralizada a fim de avaliar a implementação dessa recomendação;

104.5. A atuação do TCU em processo único, monitorando a implementação do item 9.2.1 de forma agregada, evita a duplicidade de esforços entre esta Corte e a SGD/MGI.

105. *Dessa forma, optou-se por realizar o monitoramento da recomendação 9.2.1 de forma consolidada, utilizando os dados coletados pela SGD/MGI sobre a implementação do Framework PPSI pelas organizações do Sisp.*

106. *Quanto ao critério de análise, destaca-se que o segmento de segurança da informação do Framework PPSI é fundamentado no CIS Controls. Este é composto por 153 medidas, divididas em 18 controles e categorizadas em três Grupos de Implementação (IGs), que visam à mitigação de vulnerabilidades, dos ataques mais comuns aos mais avançados. O primeiro grupo (IG1), denominado*

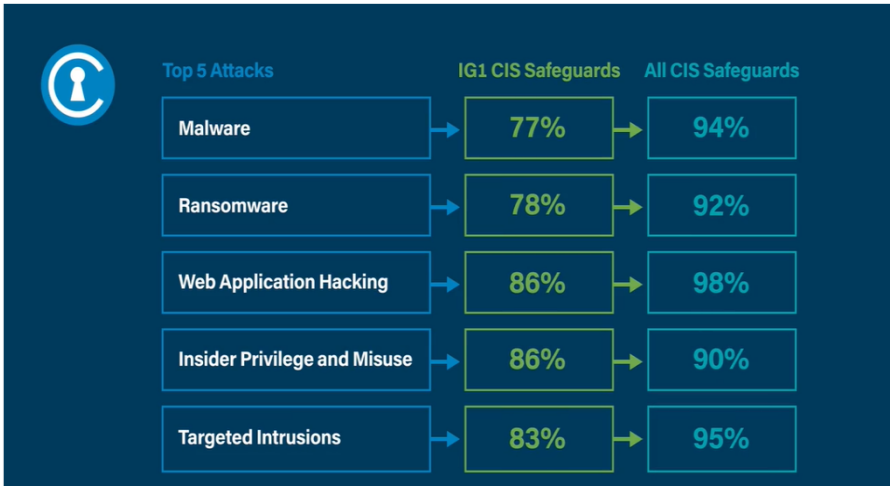
Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

'higiene cibernética', é formado por 56 medidas básicas, concebidas para instituições com diferentes níveis de maturidade e recursos.

107. *O Framework PPSI (tanto na versão 1.0 quanto na 2.0) incorporou integralmente o CIS Controls. Ajustes pontuais foram realizados apenas na descrição das medidas, visando ao alinhamento com a legislação e a literatura brasileiras.*

108. *A versão 1.3 do Guia do PPSI reconhecia o IG1 como um parâmetro de excelência para a priorização de medidas e propunha que as instituições públicas, independentemente da complexidade do ambiente tecnológico, deveriam adotar as 56 medidas do IG1 do CIS (peça 3, p. 10). Embora portarias da SGD/MGI tenham estabelecido critérios próprios de priorização em momentos distintos, a equipe de auditoria, em fiscalização pretérita, utilizou a implementação do IG1 como benchmark para concluir que as organizações do Sisp estavam aquém do esperado, visto que o IG1 se correlaciona diretamente à proteção contra os ataques cibernéticos mais comuns (peça 3, p. 8-9):*

Figura 3 - Medidas de SI do IG1 e a respectiva proteção contra os ataques mais comuns



Fonte: https://www.cisecurity.org/controls/v8, em 13/8/2024

109. *Portanto, para fins deste monitoramento, será utilizado o conjunto das 56 medidas de segurança do IG1 como parâmetro para verificar se as organizações do Sisp implementaram os controles necessários para reduzir o risco de ataques cibernéticos a um nível aceitável para as políticas públicas que executam.*

110. *Feitos esses esclarecimentos, passa-se à análise da implementação da recomendação.*

111. *A forma de avaliar e pontuar as medidas de segurança mudou no PPSI 2.0. Anteriormente, avaliava-se uma medida de segurança com a pontuação máxima se fosse implementada integralmente em mais de 50% de todos os ativos. No PPSI 2.0, para atingir a pontuação máxima, exige-se que a implementação da medida atenda mais de 80% do seu propósito e seja monitorada e revisada continuamente de forma sistemática, com base em métricas quantitativas, possuindo mecanismos que garantem uma implementação consistente ao longo do tempo. No caso de a implementação da medida atender mais de 80% do seu propósito, mas não for monitorada e revisada continuamente de forma sistemática, avalia-se com a pontuação de 0.75. Dessa forma, considera-se neste trabalho que atingir o nível Completo ou Aprimorado significa implementar a medida de segurança.*

112. *Apesar de nenhuma organização atender aos grupos de implementação IG1, IG2 ou IG3, verifica-se que houve uma melhora em cada uma das 56 medidas de segurança do IG1. Da mesma forma, o número de organizações que implementavam 90% do IG1 saiu de 2 para 12 organizações. E a quantidade que implementava menos de 40% do IG1 caiu de 166 para 123 organizações.*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

113. *Assim, apesar de ter havido uma melhora no nível de implementação dos controles de segurança cibernética, nenhuma organização do Sisp ainda implementa todas as 56 medidas de segurança do IG1, que é, de acordo com o Cis Controls, o conjunto básico de medidas de segurança de defesa cibernética que todas as organizações deveriam aplicar para se protegerem contra os ataques cibernéticos mais comuns.*

114. *Ainda que a recomendação não tenha sido para que os controles do IG1 sejam implementados, mas sim que as organizações implementassem os controles com base nos riscos das políticas que conduzem, não são necessárias, neste momento, outras informações para concluir que o nível de risco está acima do aceitável em todas as organizações, independentemente da política pública que conduz. Isso porque o nível IG1 é considerado o nível mínimo de higiene cibernética, segundo os documentos do CIS Controls, exigíveis de microempresas e empresas de pequeno porte, o que obviamente não é o caso das organizações do Sisp.*

115. *Ante o exposto, será proposto considerar em implementação a recomendação 9.2 do Acórdão 2.387/2024-TCU-Plenário, de relatoria do Ministro Augusto Nardes, uma vez que existem ações em curso no sentido de implementar os controles de segurança cibernética.*

116. *Como as organizações do Sisp avançaram na implementação dos controles, e espera-se que continuem avançando, algumas podem, no próximo ciclo de monitoramento, alcançar o nível IG1 que foi adotado na auditoria inicial e neste monitoramento como referência para tratar o risco como aceitável.*

117. *A partir daí, cada organização deverá implementar os controles de segurança cibernética necessários para reduzir o risco de ataques cibernéticos ao nível aceitável para as políticas públicas que executam. Considerando a magnitude das políticas públicas federais (e até nacionais) não se espera que o nível IG1 seja suficiente para o risco ir a um nível aceitável. Entretanto, caberá à Alta Administração das organizações decidirem, com base em gestão de risco, o ponto onde a relação benefício/custo se torna desfavorável.*

118. *Para esta avaliação, as diretrizes que a SGD/MGI expede ao longo dos ciclos pode ser um balizador de decisão para a Alta Administração tomar a decisão.*

119. *Com objetivo de apoiar a SGD/MGI no acompanhamento de como as organizações avaliam os riscos cibernéticos com respeito às suas políticas públicas, a AudTI propõe recomendar que a SGD/MGI inclua nos questionários de autoavaliação de ciclos futuros item ou itens que permitam que as organizações autoavaliem se o risco de ataques cibernéticos está no nível aceitável para as políticas públicas que elas executam.*

Deliberação 9.3

> *9.3. dar ciência às 101 organizações que não responderam ao ciclo 3 do PPSI até o dia 14/8/2024 (lista no apêndice A do relatório de peça 200), com fundamento no disposto no art. 9º, I, da Resolução-TCU nº 315/2020, sobre a obrigatoriedade de enviar à SGD/MGI sua autoavaliação e plano de ação, nos prazos determinados por ela em cada ciclo de avaliação do PPSI, conforme disposto nos artigos 6º, III, 7º, I, e 8º, I, do Decreto nº 7.579/2011, c/c o disposto no art. 9º, §§ 1º e 2º, da Portaria SGD/MGI nº 852/2023;*

Situação que levou à proposição da deliberação

120. *No ciclo 3 do PPSI, a SGD/MGI oficiou as organizações do Sisp para enviarem as informações sobre sua autoavaliação e seu plano de ação até 31 de julho de 2024 (TC 010.390/2024-3, peça 63). No entanto, de acordo com informação obtida da SGD/MGI, até 14/8/2024, 101 organizações não tinham respondido ao Ofício Circular SEI 1114/2024/MGI, que solicitou a entrega desses artefatos (TC 010.390/2024-3, peças 82-83). Posteriormente, duas organizações tiveram seus nomes removidos da lista em virtude de equívoco na inclusão de seus nomes na lista das 101*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

organizações que não responderam ao ciclo 3 do PPSI até o dia 14/8/2024 (peça 9).

121. *Para resolver a falta de envio tempestivo da autoavaliação e do plano de ação previstos no PPSI à SGD/MGI, a AudTI propôs dar ciência individualmente às organizações do Sisp que não responderam ao ciclo 3 até o dia 14/8/2024 que o não envio dos documentos solicitados pela SGD/MGI em cada ciclo de avaliação do PPSI afrontava o disposto no Decreto 7.579/2011, art. 4º, II, art. 6º, III, art. 7º, I e art. 8º, I c/c Portaria-SGD/MGI 852/2023, art. 9º, §1º e §2º.*

122. *Todas as organizações do Sisp tomaram conhecimento do entendimento do TCU quanto à omissão do envio de informações à SGD/MGI, uma vez que receberam cópia do relatório, conforme item 9.6 do Acórdão 2.387/2024 – TCU – Plenário.*

Providências adotadas pelas organizações que não responderam ao ciclo 3 do PPSI

123. *Em resposta ao Ofício 11923/2026-TCU/Seproc, a SGD/MGI enviou tabela em formato digital com a informação de entrega ou não do diagnóstico e do plano de ação por todas as organizações nos ciclos 3, 4 e 5 de implementação do PPSI 1.0 e tabela com as informações de entrega do ciclo 1 do PPSI 2.0, que se encerrou em 20/3/2026 (peças 419-420). Ademais, algumas das 101 organizações apresentaram as providências adotadas sobre o item 9.3 do Acórdão 2.387/2024-TCU-Plenário.*

Análise das providências

124. *De acordo com as tabelas enviadas pela SGD/MGI, nos ciclos 4/2025, 5/2025 e 1/2026 deveriam ter sido realizadas 743 entregas do diagnóstico e do plano de ação à Secretaria. No entanto, não houve a entrega de 45 diagnósticos.*

125. *O envio da autoavaliação e do plano de ação é essencial para que a SGD/MGI monitore e aprimore a segurança da informação na Administração Pública. Nesse sentido, a omissão no envio desses dados fragiliza o diagnóstico da maturidade em segurança cibernética das organizações, comprometendo a eficácia da formulação de políticas públicas e a racionalidade na alocação de recursos orçamentários.*

126. *A não entrega dos diagnósticos e planos de ação por parte das organizações é passível de responsabilização pelo Tribunal de Contas da União (TCU). Isso porque o descumprimento das obrigações legais estabelecidas no Decreto 7.579/2011 e nas Portarias SGD/MGI 852/2023 e 9.511/2025 pode configurar omissão ou negligência na gestão pública, especialmente quando há impacto direto na governança e na segurança da informação.*

127. *Nos termos da Resolução-TCU 315/2020, a ciência expedida pelo Tribunal tem natureza declaratória e destina-se a reorientar a atuação administrativa do jurisdicionado, prevenindo a repetição de irregularidades. Desse modo, uma vez cientificado de que determinada conduta viola norma legal, regulamentar ou entendimento consolidado do TCU, o gestor que reiterar a prática poderá sujeitar-se à responsabilização, inclusive à multa prevista no art. 58, II, da Lei 8.443/1992.*

128. *Dessa forma, para garantir a apuração adequada das responsabilidades e permitir que os gestores tenham a oportunidade de apresentar justificativas, a AudTI propõe a criação de um processo apartado específico para identificar e ouvir os responsáveis pelas organizações que não realizaram a entrega dos diagnósticos e planos de ação nos ciclos 4/2025, 5/2025 e 1/2026 do PPSI, bem como o encaminhamento de todas as informações necessárias para subsidiar a instrução, incluindo os dados fornecidos pela SGD/MGI sobre as organizações inadimplentes, os registros de comunicação entre a Secretaria e os órgãos, e demais documentos pertinentes.*

129. *Esse processo deverá ser conduzido com base nos princípios da ampla defesa e do contraditório, permitindo que os gestores expliquem as razões para o novo descumprimento e apresentem eventuais documentos ou informações que possam justificar a ausência de envio. A abertura de um processo apartado também facilita a análise individualizada de cada caso, garantindo*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

maior transparência e eficiência na apuração.

130. *Por fim cabe registrar que, ante a liderança pela gestão de riscos ser responsabilidade da Alta Administração, ela é quem responde por eventual omissão que caracteriza a desconformidade com normas legais tratados neste capítulo.*

131. *O art. 14 da Portaria - SGD/MGI 9.511/2025 atribui à estrutura de governança do PPSI a responsabilidade pela gestão do framework, o que abrange o cumprimento da obrigação de envio do autodiagnóstico e do plano de trabalho prevista no art. 16 do mesmo normativo. O art. 7º define os integrantes dessa estrutura, ao passo que o art. 8º delimita as competências específicas da Alta Administração, isto é, gerir os riscos no âmbito organizacional, fornecer os recursos necessários, viabilizar a implementação da estrutura de governança e adotar decisões sobre privacidade e segurança da informação com adequado nível de relevância e prioridade. Assim, a omissão no cumprimento dessas obrigações, inclusive o não envio do autodiagnóstico, é imputável à Alta Administração, a quem incumbe assegurar o funcionamento da estrutura de governança e o atendimento aos compromissos normativos estabelecidos.*

132. *Ante o exposto, será proposto determinar a constituição de processo apartado para a apuração individualizada das responsabilidades da Alta Administração das organizações que não realizaram a entrega do diagnóstico e do plano de ação do PPSI nos ciclos 4/2025, 5/2025 e 1/2026.*

CLASSIFICAÇÃO DE PEÇAS

133. *No processo, há informações sobre a implementação ou não de medidas de segurança pelas organizações do Sisp.*

134. *O desconhecimento de terceiros sobre controles de segurança da informação contribui, ainda que em menor escala, para a eficácia desses controles (controle por obscuridade). A divulgação dessas informações poderia aumentar o risco de comprometimento da efetividade das medidas de segurança adotadas pelas organizações do Sisp.*

135. *Já o conhecimento sobre essas medidas pode ser utilizado por agentes de ameaças para planejar e executar ataques cibernéticos direcionados, colocando em risco a integridade, confidencialidade e disponibilidade de dados e sistemas governamentais críticos, o que pode colocar em risco a segurança dessas organizações, motivo pelo qual, as peças com essas informações devem ser classificadas.*

136. *Explicitando os fundamentos legais, a AudTI propõe classificar como sigiloso em grau reservado as peças 33-34, 96, 182, 191-192, 197-198, 218-222, 226, 228-229, 243-245, 278-279, 419-420, 422, 429-430 com fundamento no art. 23, III, da Lei 12.527/2011 e nos arts. 8º, § 3º, inciso I, e 9º, inciso VII, ambos da Resolução-TCU 294/2018, restringindo seu acesso a autoridades e servidores do Tribunal de Contas da União (TCU) e da Secretaria de Governo Digital do MGI, tendo em vista que a divulgação ostensiva destas informações pode colocar em risco a segurança das informações sob gestão das organizações do Sisp.*

COMENTÁRIOS DOS GESTORES

137. *Este capítulo atende ao disposto nas Normas de Auditoria do TCU, itens 144 a 148. Também atende ao disposto no art. 14 da Resolução - TCU 315, de 2020, no sentido de oportunizar aos destinatários das deliberações a apresentação de comentários sobre as propostas sugeridas, solicitando, em prazo compatível, informações quanto às consequências práticas da implementação das medidas aventadas e eventuais alternativas.*

138. *Dessa forma, a oportunidade de apresentar comentários foi viabilizada mediante o envio da instrução preliminar com as propostas de determinação ou recomendação à SGD/MGI (peça 438). Como resultado, a organização enviou documento contendo comentários sobre as conclusões do trabalho e as propostas de encaminhamento (peça 441).*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

139. *Em síntese, os comentários sugeriram (peça 441):*

139.1. distinguir os riscos que foram mitigados pela SGD/MGI, os riscos com tratamento em execução e os riscos residuais fora da governabilidade direta da SGD/MGI, ou seja, que demandam atuação das organizações do Sisp ou de outras instâncias governamentais;

139.2. considerar que a proposta de encaminhamento contida no parágrafo 119.2 (peça 435, p. 22) está incorporada e em implementação, na medida 0.13 do framework do PPSI 2.0.

140. *As alterações relativas ao primeiro item foram incorporadas na seção 'ANÁLISE DO ATENDIMENTO DAS DELIBERAÇÕES'.*

141. *Quanto à proposta de encaminhamento contida no parágrafo 119.2, a Secretaria considera o seguinte:*

> *[...] a recomendação vai ao encontro do contido no framework do PPSI 2.0, especificamente na medida 0.13 – que objetiva avaliar se 'O órgão possui um processo de gestão de riscos de segurança da informação?', conforme Guia do Framework do PPSI disponível em PPSI 2.0 — Governo Digital.*

142. *Ocorre que a resposta ao item 0.13 do questionário do PPSI 2.0 informa à SGD/MGI se a organização possui um processo de gestão de riscos, que é uma informação útil, mas diferente da informação sobre se o nível de risco da organização está no nível tolerado por ela. A primeira é pré-condição para a segunda, pois é preciso ter processos de gestão para saber o nível de risco atual. Mas o nível de risco atual não necessariamente é aceitável.*

143. *Como se trata de informação distinta, propõe-se manter a recomendação nos mesmos termos.*

CONCLUSÃO

144. *Diante do exposto, a recomendação 9.1 se encontra parcialmente implementada, uma vez que as medidas de controle adotadas pela SGD/MGI não foram suficientes para mitigar todos os riscos a níveis aceitáveis.*

145. *A recomendação 9.2 se encontra em implementação. Houve uma melhora na implementação nos controles de segurança cibernética, no entanto nenhuma organização atende ao grupo de implementação IG1, que é o conjunto básico de medidas de segurança de defesa cibernética que todas as organizações deveriam aplicar para se protegerem contra os ataques cibernéticos mais comuns.*

146. *Ademais, em virtude da não entrega do diagnóstico e do plano de ação à SGD/MGI por organizações do Sisp, sugere-se a criação de um processo apartado específico para apurar responsabilidades pela não entrega dos diagnósticos e respectivos planos de ação nos ciclos 4/2025, 5/2025 e 1/2026 do PPSI.*

147. *Com objetivo de apoiar a SGD/MGI no acompanhamento de como as organizações avaliam os riscos cibernéticos com respeito às suas políticas públicas, a AudTI propõe recomendar que a Secretaria inclua, nos questionários de autoavaliação de ciclos futuros, um ou mais itens que permitam que as organizações autoavaliem se o risco de ataques cibernéticos está no nível aceitável para preservar a adequada entrega dos serviços e das políticas públicas sob sua responsabilidade.*

148. *Ademais, o monitoramento do item 9.2.2 do Acórdão 2.387/2024-TCU-Plenário será realizado no próximo ciclo de monitoramento, visto que a informação necessária constará dos próximos levantamentos do PPSI.*

PROPOSTA DE ENCAMINHAMENTO

149. *Ante o exposto, submetem-se os autos para consideração superior com as seguintes propostas:*

149.1. considerar parcialmente implementada a recomendação 9.1 e em implementação a recomendação 9.2.1 do Acórdão 2.387/2024-TCU-Plenário;

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

149.2. Recomendar, com fundamento no art. 11 da Resolução-TCU 315/2020, à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos que inclua, nos questionários de autoavaliação de ciclos futuros do PPSI, um ou mais itens que permitam que as organizações autoavaliem se o risco de ataques cibernéticos está no nível aceitável para preservar a adequada entrega dos serviços e das políticas públicas sob sua responsabilidade;

149.3. Determinar a constituição de processo apartado, com fulcro no art. 43 da Resolução - TCU 259/2014, para a apuração individualizada das responsabilidades da Alta Administração das organizações que não realizaram a entrega do diagnóstico e do plano de ação do PPSI nos ciclos 4/2025, 5/2025 e 1/2026, facultando-se a utilização de todos os elementos probatórios constantes destes autos, incluindo os dados fornecidos pela SGD/MGI e os registros de comunicação, para subsidiar a instrução e a eventual audiência dos responsáveis;

149.4. Classificar como sigilosas em grau reservado, com fundamento no art. 23, VII, da Lei 12.527/2011 e nos arts. 8º, § 3º, inciso I e 9º, inciso VII, ambos da Resolução-TCU 294/2018, as peças 33-34, 96, 182, 191-192, 197-198, 218-222, 226, 228-229, 243-245, 278-279, 419-420, 422, 429-430, restringindo seu acesso a autoridades e servidores do Tribunal de Contas da União (TCU) e da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), tendo em vista que a divulgação ostensiva destas informações pode colocar em risco a segurança das organizações do Sisp;

149.5. Informar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI) do acórdão que vier a ser proferido, destacando que o relatório, o voto e os apêndices que fundamentam a deliberação ora encaminhada poderão ser acessados por meio do endereço eletrônico www.tcu.gov.br/acordaos;

149.6. Nos termos do art. 8º da Resolução - TCU 315, de 2020, fazer constar, na ata da sessão em que estes autos forem apreciados, comunicação do Relator ao colegiado no sentido de autorizar que o monitoramento da recomendação proposta nesta instrução bem como a do item 9.2.2 do Acórdão 2.387/2024-TCU-Plenário ocorram em conjunto;

149.7. Apensar os presentes autos ao TC 010.390/2024-3, processo que originou o acórdão ora monitorado."

É o Relatório.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167365.

VOTO

Trata-se de monitoramento das recomendações constantes dos itens 9.1, 9.2.1, e 9.2.2 do Acórdão 2.387/2024-TCU-Plenário, de minha relatoria, proferido no âmbito do TC 010.390/2024-3, que abriga auditoria operacional realizada pela Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI) com o objetivo de avaliar em que medida os controles de cibersegurança e de segurança da informação implementados pelas organizações integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) se encontravam aderentes às boas práticas, especialmente às previstas no Programa de Privacidade e Segurança da Informação (PPSI).

2. Naquela oportunidade, o Tribunal recomendou à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI):

9.1. recomendar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) que aperfeiçoe o PPSI, gerenciando os riscos constantes do apêndice D do relatório de peça 200, adotando as medidas de controle que estiverem sob sua governabilidade e orientando as organizações do Sisp quando as medidas estiverem na respectiva esfera de governabilidade;

3. Nos subitens 9.2.1 e 9.2.2, recomendou às organizações que compõem o Sisp:

9.2. recomendar a cada uma das organizações do Sisp relacionadas no apêndice E do relatório de peça 200 que:

9.2.1. adotem medidas para implementar os controles de segurança cibernética necessários para reduzir o risco de ataques cibernéticos ao nível aceitável para as políticas públicas que executam, utilizando como referencial as diretrizes expedidas pela SGD/MGI por meio do PPSI, de acordo com o art. 8º da Portaria-SGD/MGI nº 852/2023;

9.2.2. envidem esforços para que o processo de gestão de riscos decorrentes de ataques cibernéticos seja liderado explicitamente pela sua alta administração, alinhado ao previsto no art. 17 do Decreto nº 9.203/2017;

4. No presente monitoramento, a AudTI examinou as providências adotadas pela SGD/MGI e pelas organizações do Sisp, com especial atenção aos riscos identificados na fiscalização original. Verificou que parte relevante das deficiências apontadas foi objeto de medidas de controle, inclusive com a instituição do PPSI 2.0, por meio da Portaria SGD/MGI 9.511/2025, e a edição da Instrução Normativa SGD/MGI 4/2026, que disciplina o ciclo de implementação de 2026.

5. A unidade técnica concluiu, ao final, que a recomendação constante do subitem 9.1 se encontra parcialmente implementada e que aquela constante do subitem 9.2.1 está em implementação (a recomendação constante do subitem 9.2.2. será avaliada no próximo ciclo de monitoramento, visto que a informação necessária constará dos próximos levantamentos do PPSI).

6. Em conclusão, propõe a AudTI a expedição de nova recomendação à SGD/MGI, a constituição de processo apartado para apuração das responsabilidades pela ausência de entrega de diagnósticos e planos de ação do PPSI e o tratamento sigiloso de determinadas peças dos autos.

7. Feito esse breve relato, passo a decidir.

8. Acompanho, em essência, as conclusões da unidade técnica, cujos fundamentos adoto como razões de decidir, sem prejuízo das considerações que passo a expor.

9. O presente monitoramento revela evolução concreta na estruturação do PPSI. Entre as medidas adotadas pela SGD/MGI, destacam-se a criação de indicadores de acompanhamento da maturidade do programa, a definição de atribuições para a alta administração das organizações, o aperfeiçoamento da escala de medição das medidas de segurança, a disponibilização do SisPPSI e o reforço da disciplina normativa relativa à gestão de riscos de privacidade e segurança da informação.

10. Assim, foram considerados mitigados, entre outros, os riscos relacionados à insuficiência de indicadores e metas, à ausência de atribuição explícita de responsabilidade à alta administração, à antiga escala de medição das medidas de segurança, à inexistência de pré-preenchimento com as

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167367.

respostas de ciclos anteriores, ao desconhecimento do modelo de três linhas de defesa e à utilização de planilhas eletrônicas para o preenchimento das avaliações.

11. O resultado não significa, contudo, que os riscos identificados na auditoria original tenham sido integralmente superados. Persistem, por exemplo, relevantes limitações de pessoal nas áreas de tecnologia da informação, tanto na SGD/MGI quanto nas organizações do Sisp.

12. A própria Secretaria reconhece que o ingresso de novos servidores não foi suficiente para suprir a demanda, havendo necessidade de novos concursos e de ampliação da estrutura da carreira de Analista em Tecnologia da Informação. Trata-se, portanto, de problema estrutural que não se encontra inteiramente sob a governabilidade imediata da SGD/MGI.

13. Situação semelhante ocorre com a elevada rotatividade dos profissionais de tecnologia da informação, cuja mitigação depende, entre outros fatores, da capacidade de retenção de servidores e da atratividade da carreira. A propósito, a própria unidade técnica registra que o Acórdão 1.475/2026-TCU-Plenário já recomendou ao Ministério da Gestão e da Inovação em Serviços Públicos a adoção de medidas concretas para enfrentar os desafios relacionados à atratividade da carreira de Analista em Tecnologia da Informação.

14. Também permanecem situações que extrapolam a atuação direta da SGD/MGI. É o caso da ausência de designação de gestor de segurança da informação em quinze organizações do Sisp, embora tenha havido expressiva melhora em relação ao cenário encontrado na auditoria original. Como observado pela unidade técnica, a adoção dessa providência incumbe às próprias organizações, e não à Secretaria de Governo Digital.

15. Igualmente subsistem riscos relacionados à participação da Comissão de Coordenação do Sisp na definição dos controles priorizados, à ausência de evidências obrigatórias sobre a implementação dos controles, à inexistência de metodologia formal de agrupamento das organizações, à insuficiência de mecanismos de ***enforcement*** e à disponibilidade de recursos financeiros para a implementação das medidas priorizadas.

16. Nesse contexto, considero adequada a conclusão da AudTI de que a recomendação constante do subitem 9.1 deve ser classificada como parcialmente implementada. As medidas adotadas pela SGD/MGI demonstram evolução importante do programa e mitigaram diversos riscos, mas não foram suficientes para reduzi-los todos a níveis aceitáveis.

17. Quanto à recomendação constante do subitem 9.2.1, a situação também merece ser vista sob perspectiva evolutiva. O monitoramento identificou melhora na implementação dos controles de segurança cibernética pelas organizações do Sisp. Todavia, nenhuma das organizações avaliadas alcançou o nível IG1, utilizado na auditoria original como referência mínima para o conjunto básico de medidas de defesa cibernética contra os ataques mais comuns.

18. Por essa razão, não há fundamento para considerar cumprida a recomendação. Existem ações em curso, mas o objetivo de reduzir os riscos de ataques cibernéticos a níveis aceitáveis para as políticas públicas executadas pelas organizações ainda não foi alcançado. Correta, portanto, a classificação da recomendação como em implementação.

19. Considero igualmente pertinente a nova recomendação proposta pela unidade técnica, para que a SGD/MGI inclua, nos questionários de autoavaliação de ciclos futuros do PPSI, item ou itens que permitam às organizações avaliar se o risco de ataques cibernéticos se encontra em nível aceitável para a adequada prestação dos serviços e execução das políticas públicas sob sua responsabilidade.

20. A providência tem utilidade que ultrapassa a simples aferição da existência de processos formais de gestão de riscos. Como bem observado pela AudTI, informar se a organização possui um processo de gestão de riscos é diferente de aferir se o nível de risco efetivamente identificado se encontra dentro do limite que a própria organização considera aceitável. A primeira informação constitui condição para a segunda, mas não a substitui.

21. Passo, então, à questão relativa às organizações que deixaram de encaminhar à SGD/MGI os diagnósticos e planos de ação previstos nos ciclos mais recentes do PPSI.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167367.

22. A unidade técnica verificou que, nos ciclos 4/2025, 5/2025 e 1/2026, de um total de 743 entregas esperadas, 45 diagnósticos não foram encaminhados. Trata-se de informação relevante, pois a ausência desses dados compromete a capacidade da Secretaria de acompanhar a maturidade em segurança cibernética das organizações do Sisp e, consequentemente, de formular políticas e direcionar recursos de maneira adequada.

23. Não se trata, portanto, de mera deficiência formal. O envio do autodiagnóstico e do plano de ação constitui elemento essencial do modelo de governança concebido para o PPSI, permitindo ao órgão central conhecer o estágio de implementação dos controles e orientar as organizações quanto às medidas necessárias.

24. Afigura-se, assim, adequada a proposta de constituição de processo apartado para a apuração individualizada das responsabilidades dos integrantes da alta administração das organizações que deixaram de realizar as entregas. A medida permitirá que cada caso seja examinado de forma individualizada, assegurando-se aos responsáveis o contraditório e a ampla defesa, inclusive quanto às circunstâncias eventualmente justificadoras da omissão.

25. Ressalto que essa providência não importa, neste momento, em juízo definitivo acerca da responsabilidade dos gestores. O que se mostra necessário é instaurar procedimento próprio que permita identificar os responsáveis, examinar as circunstâncias de cada omissão e, se for o caso, promover a respectiva audiência.

26. Quanto à recomendação 9.2.2, a unidade técnica informa que seu monitoramento, como antes mencionado, será realizado no próximo ciclo, uma vez que as informações necessárias à sua avaliação constarão dos próximos levantamentos do PPSI. Considero adequada essa providência, evitando-se antecipar conclusão sobre questão que ainda não dispõe dos elementos necessários para exame.

27. Por fim, acompanho a proposta de classificação, em grau reservado, das peças que contêm informações acerca da implementação das medidas de segurança pelas organizações do Sisp. Conforme apontado pela unidade técnica, a divulgação ostensiva de tais informações pode fornecer a terceiros elementos capazes de facilitar a identificação de vulnerabilidades e, consequentemente, aumentar os riscos de comprometimento de sistemas e dados governamentais.

28. Considero, portanto, que o monitoramento cumpriu adequadamente sua finalidade, ao demonstrar evolução concreta do PPSI, sem perder de vista os riscos que ainda demandam tratamento. A classificação diferenciada das recomendações permite, a meu ver, retratar com maior precisão esse estágio de maturidade: alguns riscos foram mitigados; outros permanecem em tratamento; e há, ainda, situações cuja superação depende de providências de outras organizações ou de decisões que extrapolam a governabilidade imediata da SGD/MGI.

Ante o exposto, acolho as conclusões e propostas da Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI) e voto no sentido de que o Tribunal adote o Acórdão que ora submeto à deliberação deste Colegiado.

TCU, Sala das Sessões, em 14 de outubro de 2026.

Ministro JOÃO AUGUSTO RIBEIRO NARDES
Relator

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167367.

ACÓRDÃO Nº 2829/2026 – TCU – Plenário

1. Processo nº TC 005.618/2025-8.
2. Grupo I – Classe de Assunto: V – Monitoramento.
3. Interessados/Responsáveis: não há.
4. Unidades Jurisdicionadas: Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e outros.
5. Relator: Ministro João Augusto Ribeiro Nardes.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI).
8. Representação legal: não há.

9. Acórdão:

VISTOS, relatados e discutidos estes autos de monitoramento das determinações contidas nos subitens 9.1 e 9.2.1 do Acórdão 2.387/2024-TCU-Plenário, proferido nos autos do TC-010.390/2024-3, que abriga relatório de auditoria operacional com o objetivo de avaliar em que medida os controles de cibersegurança e de segurança da informação implementados pelas organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) estão de acordo com as boas práticas, em especial comparados ao previsto no Framework de Privacidade e Segurança da Informação (Portaria-SGD/MGI 852/2023);

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, por unanimidade, ante as razões expostas pelo Relator, em:

9.1. considerar parcialmente implementada a recomendação constante do subitem 9.1 do Acórdão 2.387/2024-TCU-Plenário e em implementação aquela constante do subitem 9.2.1;

9.2. recomendar, com fundamento no art. 11 da Resolução-TCU 315/2020, à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos que inclua, nos questionários de autoavaliação de ciclos futuros do PPSI, um ou mais itens que permitam que as organizações autoavaliem se o risco de ataques cibernéticos está no nível aceitável para preservar a adequada entrega dos serviços e das políticas públicas sob sua responsabilidade;

9.3. determinar a constituição de processo apartado, com fulcro no art. 43 da Resolução - TCU 259/2014, para a apuração individualizada das responsabilidades da Alta Administração das organizações que não realizaram a entrega do diagnóstico e do plano de ação do PPSI nos ciclos 4/2025, 5/2025 e 1/2026, facultando-se a utilização de todos os elementos probatórios constantes destes autos, incluindo os dados fornecidos pela SGD/MGI e os registros de comunicação, para subsidiar a instrução e a eventual audiência dos responsáveis;

9.4. classificar como sigilosas, em grau reservado, com fundamento no art. 23, VII, da Lei 12.527/2011 e nos arts. 8º, § 3º, inciso I e 9º, inciso VII, ambos da Resolução-TCU 294/2018, as peças 33-34, 96, 182, 191-192, 197-198, 218-222, 226, 228-229, 243-245, 278-279, 419-420, 422, 429-430, restringindo seu acesso a autoridades e servidores do Tribunal de Contas da União (TCU) e da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), tendo em vista que a divulgação ostensiva destas informações pode colocar em risco a segurança das organizações do Sisp;

9.5. autorizar que o monitoramento da recomendação constante no subitem 9.2 acima ocorra em conjunto com aquela constante no subitem 9.2.2. do Acórdão 2.387/2024-TCU-Plenário, que será avaliada no próximo ciclo de monitoramento;

9.6. dar ciência deste acórdão à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI) e aos demais interessados; e

9.7. apensar estes autos ao TC 010.390/2024-3, processo que originou o acórdão ora monitorado.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167379.

10. Ata n° 40/2026 – Plenário.
11. Data da Sessão: 14/10/2026 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-2829-40/26-P.
13. Especificação do quórum:
13.1. Ministros presentes: Jorge Oliveira (na Presidência), Walton Alencar Rodrigues, Augusto Nardes (Relator), Jhonatan de Jesus, Odair Cunha e Rodrigo Pacheco.
13.2. Ministro-Substituto convocado: Augusto Sherman Cavalcanti.
13.3. Presidente não votou (Resolução-TCU 375/2025, art. 3º).

(Assinado Eletronicamente)
JORGE OLIVEIRA
Vice-Presidente, no exercício da Presidência

(Assinado Eletronicamente)
AUGUSTO NARDES
Relator

Fui presente:

(Assinado Eletronicamente)
CRISTINA MACHADO DA COSTA E SILVA
Procuradora-Geral

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 81167379.