GRUPO I – CLASSE V – Plenário
TC 017.092/2023-0.
Natureza: Relatório de Acompanhamento.
Órgão: Tribunal de Contas da União.
Representação legal: não há.

SUMÁRIO: ACOMPANHAMENTO. CONSOLIDAÇÃO DOS RESULTADOS DAS AUDITORIAS OPERACIONAIS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA NO ÂMBITO DA ESTRATÉGIA DO PRIMEIRO CICLO DO PROTEGE-TI, REALIZADAS NOS EXERCÍCIOS 2023 E 2024, EM ORGANIZAÇÕES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. CIÊNCIA.

RELATÓRIO

Trata-se de fiscalização, na modalidade de acompanhamento, realizada pela Secretaria de Controle Externo de Governança, Inovação e Transformação Digital do Estado (SecexEstado), cujo relatório[1], com proposta em uníssono da referida unidade especializada[2], transcrevo parcialmente a seguir:

> "1 **Introdução**
>
> 1. O PROTEGE-TI **é a estratégia de controle externo** da AudTI em segurança da informação e cibernética, que tem o propósito de 'tornar seguro o ambiente digital sob a governabilidade do Brasil'.
>
> 2. A estratégia é **ágil** e **executada em ciclos anuais** orientados pela **priorização de objetos** classificados por **categorias de riscos**. As categorias de riscos atualmente englobam: a) riscos **estratégicos**, como a atual situação da Política Nacional de Cibersegurança; b) riscos **táticos**, como o nível de maturidade em cibersegurança das organizações do poder executivo federal; c) riscos **operacionais**, decorrentes da insuficiência de controles técnicos que protejam as organizações dos principais vetores de ataques cibernéticos, como aqueles utilizados nos ataques ao STJ em 2020, que impactaram negativamente o andamento dos processos durante alguns meses; ao Ministério da Saúde em 2021, que paralisou a emissão dos cartões de vacinação contra Covid por cerca de um mês (TC 019.703/2023-6, Relator Min. Augusto Nardes); ao Sistema Integrado de Administração Financeira (Siafi), com desvios de recursos (TC 024.560/2024-3, Relator Min. Bruno Dantas); e aos sistemas do Instituto Nacional do Seguro Social (INSS), com vazamento de dados de milhões de beneficiários.
>
> 3. O primeiro ciclo dessa estratégia iniciou-se no plano de controle 2023/2024, autorizado por meio do Acórdão 1.104/2023-TCU-Plenário (Rel. Ministro Aroldo Cedraz).
>
> 4. O foco desse ciclo foi a redução de riscos **operacionais** no caminho de ataque de *ransomware* e engloba aspectos relacionados a acesso inicial, gestão de incidentes, configurações do ambiente computacional e procedimentos para realização e restauração de cópias de segurança de ambientes críticos. O trabalho consistiu, inicialmente, em seis fiscalizações:
>
> 4.1. F1 – Auditoria dos Controles de Segurança dos Servidores *Web*, e-mail e DNS (*Domain Name System*);
>
> 4.2. F2 – Auditoria Sobre o Vetor de Ataque *Phishing*;

[1] Peça 6.

[2] Peças 7-8.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

4.3. F3 – Auditoria de Gestão de Controle de Acesso e Credenciais

4.4. F4 – Auditoria de Gestão do *Active Directory* - Serviços de Domínio (AD-DS);

4.5. F5 – Auditoria em Gestão de Resposta a Incidentes de Segurança da Informação;

4.6. F6 – Auditoria de Gestão de Cópias de Segurança.

5. Durante a execução do ciclo, optou-se por terminar o acompanhamento sem a realização da F3 – Gestão de controle de acesso e credenciais. O tema da F3 foi abordado em duas outras fiscalizações do TCU: a inspeção do Siafi (TC 024.560/2024-3, Rel. Min. Bruno Dantas) e a auditoria do portal Gov.br (TC 015.635/2025-2, Rel. Min. Aroldo Cedraz). À época da elaboração deste relatório, a primeira fiscalização sobre o tema da F3 ainda estava pendente de julgamento pelo Plenário do TCU, enquanto a segunda ainda estava em fase de execução.

6. A primeira fiscalização (inspeção) foi desenhada para responder questionamentos oriundos de representação do Ministério Público junto ao TCU e solicitação do Congresso Nacional acerca do incidente de segurança da informação ocorrido em março de 2024 no Siafi. Seu escopo foi não só avaliar os controles técnicos na área de gestão de identidades e autenticação do Siafi, como também esclarecer pontos acerca do mencionado incidente de segurança.

7. Devido a sua peculiaridade (origem distinta e uma só organização fiscalizada, a STN) e a sensibilidade de seu objeto (incidente de segurança da informação que ocorreu), optou-se por não incluir esse trabalho nesse consolidador.

8. Já a segunda fiscalização tem foco na identificação e autenticação segura dos usuários do Gov.br e ainda está em andamento, por isso não foi contemplada nesse relatório.

9. Na Figura 1, as fiscalizações estão identificadas como ‘F1’ a ‘F6’.

Figura 1 - Anatomia de um ataque de *ransomware*

[...]

Fonte: elaborada pela equipe de auditoria.

10. O **objetivo** do presente relatório é consolidar os resultados de auditorias operacionais de segurança da informação e segurança cibernética, no âmbito da estratégia do primeiro ciclo do PROTEGE-TI, que foram realizadas ao longo dos exercícios 2023 e 2024, em organizações da Administração Pública Federal.

2 O QUE É RANSOMWARE?

11. ***Ransomware*** é um tipo de *malware* (*software* malicioso) que sequestra os dados de um sistema ou dispositivo, criptografando-os e exigindo um resgate (do inglês, *ransom*) para descriptografar e restaurar o acesso aos dados. Em outras palavras, trata-se de um tipo de ataque cibernético onde os agentes de ameaças (os chamados *hackers*) impedem o acesso do proprietário dos dados aos seus próprios dados, geralmente por meio de criptografia forte, e então exigem um pagamento para liberar a chave de acesso. Mesmo em caso de pagamento, não há garantias que a vítima terá acesso integral aos seus dados. Esses ataques podem causar interrupções significativas nos serviços e resultar em perdas financeiras substanciais.

12. Em 2022, o Brasil foi o 2º maior país alvo de ataques de *ransomware* do mundo, ficando atrás somente dos Estados Unidos, sendo a vítima preferencial na América Latina. Além disso, a mídia especializada também reporta que, em 2023, quase metade dos ataques de *ransomware* (46%) foi bem-sucedido no Brasil.

13. Nos últimos anos, diversas organizações públicas do governo federal foram alvos de ataques cibernéticos do tipo *ransomware*. Segundo informações da mídia, esses ataques têm sido especialmente frequentes, afetando uma variedade de organizações públicas e privadas. Entre as organizações públicas atacadas, está a Secretaria do Tesouro Nacional (STN) em agosto de 2021 e o Ministério da Saúde em dezembro de 2021. Além dessas, outras instituições como a Agência Nacional de Águas (ANA) e a Fiocruz também sofreram ataques semelhantes. Outro caso notável foi o incidente significativo de *ransomware* que

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

ocorreu na Presidência da República em 11 de novembro de 2022, responsável por comprometer 192 estações de trabalho dos usuários.

14. Para realizar um ataque de *ransomware*, o primeiro passo do atacante, conhecido também como agente de ameaça, é obter acesso inicial ao ambiente tecnológico da organização alvo. Isso pode ocorrer por meio de diferentes formas, conhecidas como vetores de ataque, tais como:

14.1. Exploração de vulnerabilidades e falhas de configuração de serviços expostos à Internet;

14.2. Realização de ataques de *phishing* para obtenção de credenciais ou acessos a sistemas internos;

14.3. Implantação de *malware* diretamente nos ativos da organização;

14.4. Comprometimento de prestadores de serviço, conhecidos como terceiros confiáveis.

15. As fiscalizações *F1 – Auditoria dos Controles de Segurança dos Servidores Web, e-mail e DNS* e *F2 – Auditoria Sobre o Vetor de Ataque Phishing* tiveram como objetivo promover a melhoria na gestão de riscos dos vetores de ataque descritos nos parágrafos 14.1 e 14.2, respectivamente.

16. Uma vez obtido o acesso inicial, o atacante realiza um reconhecimento do ambiente, etapa conhecida como enumeração. A partir dessa análise, ele busca vulnerabilidades e tenta obter novas credenciais, visando ampliar seu acesso a outros sistemas e ativos, prática denominada movimentação lateral. Esse processo foi objeto da fiscalização *F4 – Auditoria de Gestão do Active Directory - Serviços de Domínio (AD-DS)*.

17. Caso a movimentação lateral tenha sucesso, o atacante compromete o ambiente e implanta o *ransomware*, criptografando os dados da organização alvo. A vítima então se depara com duas alternativas:

17.1. Pagar o resgate exigido, sem qualquer garantia de que os dados serão efetivamente recuperados ou de que o atacante não explorará novamente as mesmas vulnerabilidades no futuro;

17.2. Restaurar os dados a partir de suas cópias de segurança confiáveis.

18. A primeira alternativa é inadmissível no âmbito da Administração Pública Federal, visto que o pagamento de resgate a criminosos viola os princípios da legalidade e da moralidade administrativa (art. 37, *caput*, da Constituição Federal de 1988).

19. Assim, a recuperação dos serviços depende diretamente da existência e da eficácia das cópias de segurança (*backups*), tema tratado na fiscalização *F6 – Auditoria de Gestão de Cópias de Segurança*.

20. Para que uma organização esteja preparada para prevenir e responder a ataques, é essencial que disponha de normas, processos e procedimentos bem definidos, além de soluções tecnológicas (hardware, software e serviços), que resultem na implementação de controles eficazes para tratamento dos riscos cibernéticos. Entretanto, mesmo com controles em vigor, é possível que incidentes ocorram. Nesses casos, a organização deve ter capacidade para detectá-los, responder adequadamente e aprender com seus próprios erros. Essa capacidade foi analisada na *F5 – Auditoria em Gestão de Resposta a Incidentes de Segurança da Informação*.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

3 PROTEGE-TI 2023/2024: AUDITORIAS REALIZADAS

3.1 QUADRO RESUMO DAS AUDITORIAS REALIZADAS

21. A tabela abaixo registra o quadro resumo das onze auditorias realizadas:

Fiscalização	Processo (TC)	Acórdão
F1: Auditoria dos Controles de Segurança dos Servidores Web, e-mail e DNS	017.413/2023-0	523/2024- Plenário
F2: Auditoria Sobre o Vetor de Ataque *Phishing*	019.227/2023-0	2079/2024-Plenário
	019.228/2023-6	2080/2024-Plenário
	019.229/2023-2	2081/2024-Plenário
F4: Auditoria de Gestão do *Active Directory* - Serviços de Domínio (AD-DS)	039.230/2023-6	750/2025-Plenário
	039.231/2023-2	751/2025-Plenário
	039.233/2023-5	752/2025-Plenário
F5: Auditoria em Gestão de Resposta a Incidentes de Segurança da Informação	039.955/2023-0	509/2025-Plenário
	039.956/2023-7	510/2025-Plenário
F6: Auditoria de Gestão de Cópias de Segurança	040.034/2023-2	639/2025-Plenário
	040.039/2023-4	537/2025-Plenário

22. O método de auditoria das fiscalizações está no **Error! Reference source not found.**

3.2 F1: AUDITORIA DOS CONTROLES DE SEGURANÇA DOS SERVIDORES *WEB*, E-MAIL E DNS

Objetivo da fiscalização

23. O **objetivo** da **F1** foi promover a melhoria na gestão de riscos de segurança da informação nas organizações públicas no contexto dos serviços de hospedagem *web*, *e-mail* e resolução de nomes (DNS), acessíveis pela internet. A fiscalização, do tipo auditoria operacional, testou milhares de domínios de organizações públicas dos três poderes da União, das três esferas de Governo, para identificar se existem ou não falhas de configuração em servidores *web*, *e-mail* e DNS (*Domain Name Service*) acessíveis pela internet e que podem ser exploradas por agentes de ameaça. Os testes foram realizados com apoio da ferramenta 'TOP', disponibilizada pelo NIC.BR (http://top.nic.br).

Por que o TCU fiscalizou

24. Mais de 80% dos ataques de *ransomware* podem ser atribuídos a erros de configuração em softwares e em dispositivos, segundo o relatório *Microsoft Cyber Signals* 2022. Além disso, de acordo com a última edição do OWASP Top 10, documento padrão que promove conscientização entre desenvolvedores e profissionais de segurança sobre os riscos mais críticos para aplicativos web, as configurações inseguras são classificadas como o quinto problema mais comum em termos de riscos à segurança.

O que o TCU encontrou

25. Foram identificados sete riscos cuja consolidação sinalizou que poderá ocorrer a manipulação de tráfego de rede, comprometimento de contas de usuários, roubo, vazamento e perda de dados ou mesmo disrupção dos sistemas de organizações públicas.

26. O escopo da auditoria incluiu 29 testes *web* e 27 testes de *e-mail* realizados pela ferramenta TOP do Nic.br, adaptada utilizando como base o *site* internet.nl, que é uma iniciativa da holandesa *Internet Standards Platform*.

26.1. Os testes de *web* foram agrupados nas seguintes categorias:

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

26.1.1. Endereço IP moderno (IPv6);

26.1.2. Nome de domínio assinado (DNSSEC);

26.1.3. Conexão segura (HTTPS); e

26.1.4. Cabeçalhos de segurança HTTP.

26.2. Por outro lado, os testes de *e-mail* foram agrupados nas seguintes categorias:

26.2.1. Endereço IP moderno (IPv6);

26.2.2. Nomes de domínio assinados (DNSSEC);

26.2.3. Marcas de autenticidade contra *phishing* (DMARC, DKIM e SPF); e

26.2.4. Conexão segura com servidor de *e-mail* (STARTTLS e DANE).

27. As conclusões parciais obtidas durante a fiscalização (setembro/2023) sinalizam deficiência na configuração de controles recomendados pelas boas práticas para serviços de hospedagem *web*, *e-mail* e DNS, expondo a maioria das organizações e seus clientes a diversos ataques cibernéticos, em especial:

27.1. Poucos domínios testados (2%) estavam com nível de risco baixo quanto à confidencialidade, que pode ser obtida por meio da implementação de conexão segura pela *web*;

27.2. Poucos domínios testados estavam com nível de risco baixo quanto à confidencialidade e a integridade, que podem ser obtidas por meio da implementação de criptografia em tráfego pela *web* e por *e-mail* (6% e 5%, respectivamente);

27.3. Muitos dos domínios testados (84%) estavam com nível de risco alto para ataques contra as aplicações hospedadas nos seus servidores *web*, por não implementarem nenhum dos quatro cabeçalhos testados;

27.4. Muitos domínios testados estavam com nível de risco alto para ataques ao serviço de resolução de nomes, que apoiam tanto os serviços *web* quanto os serviços de *e-mail* (81% e 86%, respectivamente);

27.5. Poucos dos domínios testados estavam com nível de risco baixo com relação à implementação de todos os aspectos essenciais do protocolo moderno IPv6, tanto os serviços *web* quanto os serviços de *e-mail* (8% em ambos os casos);

27.6. Poucos dos domínios avaliados (8%) implementavam as proteções contra *phishing* testadas, estando com nível de risco baixo para este tipo de ataque.

Resultado

28. A partir dos riscos identificados (parágrafo 25), foi dado conhecimento das conclusões e resultados da fiscalização a oito organizações que representam a multiplicidade de organizações detentoras dos domínios avaliados, para que avaliem, se entenderem conveniente e oportuno, a adoção de medidas e a elaboração de estratégias para orientar as organizações que se encontram na sua área de atuação sobre a gestão dos riscos decorrentes da não implantação dos controles ora analisados.

29. Além disso, foi autorizada a criação de guia (...) para orientar a tomada de decisão sobre a implementação dos controles avaliados.

Deliberação

30. A fiscalização foi apreciada e deu origem ao Acórdão 523/2024-TCU-Plenário (Rel. Min. Aroldo Cedraz).

3.3 F2: AUDITORIA SOBRE O VETOR DE ATAQUE PHISHING

Objetivo da fiscalização

31. O **objetivo** da **F2** foi promover a melhoria da gestão de riscos nas organizações públicas no contexto do vetor de ataque *phishing* por meio da avaliação de controles administrativos, técnicos e de conscientização em relação às boas práticas sobre o tema. O TCU realizou três auditorias de natureza operacional em três organizações diferentes.

Por que o TCU fiscalizou

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

32. O *phishing* é uma forma específica de ataque de engenharia social, que é uma tática utilizada por cibercriminosos (atacantes) para manipular a psicologia humana e induzir indivíduos a realizarem ações que comprometam a segurança ou divulguem informações sensíveis. É ainda a principal forma de ataque de engenharia social da atualidade, sendo a ferramenta mais usada para que atacantes ingressem na rede da organização, estabelecendo seu acesso inicial (*foothold*) para avançar e realizar o ataque de *ransomware*.

O que o TCU encontrou

33. A principal conclusão foi que existe suscetibilidade dos usuários das organizações a contribuírem, ainda que não intencionalmente, com ataques de *phishing*. Além disso, em todos os eixos avaliados foram detectadas deficiências ou oportunidades de melhoria que geram riscos relevantes relacionados ao vetor de ataque *phishing*.

34. O gráfico abaixo ilustra o grau de aderência às boas práticas das organizações auditadas:

[...]

35. O **escopo** da auditoria incluiu avaliar:

35.1. Os controles dos eixos administrativo, técnico e de conscientização existentes para mitigar o risco de ataques de *phishing*¸ conforme Figura 2:

Figura 2 - Eixos avaliados na auditoria

[...]

Fonte: elaborada pela equipe de auditoria.

35.2. Os processos de identificação e resposta a ataques de *phishing* adotados pelas organizações; e

35.3. A capacidade dos usuários das organizações auditadas de identificar e reagir adequadamente (e.g. notificar setor responsável) quando diante de *e-mails* maliciosos, por meio da realização de uma simulação de *phishing*.

36. A Figura 3 exemplifica um *e-mail* encaminhado na simulação de *phishing* realizada em uma das organizações auditadas:

Figura 3 - Template de e-mail utilizado na simulação de *phishing*

[...]

Fonte: elaborada pela equipe de auditoria.

37. Por meio dessa simulação, a equipe pôde verificar se os usuários das organizações auditadas contribuíram, ainda que não intencionalmente, com ataques de *phishing*, ao, por exemplo, clicarem em um *link* que poderia ser malicioso, fornecerem informação pessoal em um formulário que poderia ser malicioso, entre outros comportamentos.

38. As principais deficiências, oportunidades de melhoria e pontos de atenção que levaram à conclusão (parágrafo 33) estão sumarizadas a seguir:

38.1. Nas simulações de *phishing* realizadas pela equipe de auditoria, os usuários realizaram ações (clicar em *link* malicioso, forneceram informação sensível e abriram um arquivo potencialmente malicioso) que contribuiriam, ainda que não intencionalmente, para um ataque de *phishing;*

38.2. Há deficiências no programa e nas ações de conscientização para os membros da força de trabalho das organizações reconhecerem ataques de engenharia social, em especial de *phishing*, ligadas ao estabelecimento de um programa e ao direcionamento das ações;

38.3. Foram identificadas oportunidades de melhoria nos controles dos eixos administrativo e técnico, relacionadas à política de uso aceitável dos ativos e a processos de trabalho para mapeamento dos usuários expostos a maior risco de *phishing*.

Resultado

39. Diante dos resultados que lhes foram apresentados ao final da fiscalização (parágrafo 33), as três organizações auditadas enviaram à equipe Plano de Ação informando

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

como pretendiam lidar com as deficiências que entenderam ser de maior risco. O envio desses planos evidenciou que a alta gestão dessas organizações assumiram a responsabilidade pelos riscos e pretendem melhorar a gestão de risco no contexto do vetor de ataque *phishing*.

Deliberação

40. As fiscalizações foram apreciadas por meio dos Acórdãos 2.079/2024-TCU-Plenário, 2.080/2024-TCU-Plenário e 2.081/2024-TCU-Plenário (todos do Rel. Min. Aroldo Cedraz).

3.4 F4: AUDITORIA DE GESTÃO SERVIÇOS DE DOMÍNIO DO ACTIVE DIRECTORY

Objetivo da fiscalização

41. O **objetivo** da **F4** foi promover a melhoria na gestão de riscos de segurança da informação nas organizações públicas no contexto dos Serviços de Domínio do *Active Directory* (AD-DS) da Microsoft, por meio da avaliação dos controles administrativos e técnicos existentes. O TCU realizou três auditorias de natureza operacional em três organizações diferentes.

Por que o TCU fiscalizou

42. O serviço de diretório Microsoft *Active Directory* (AD) é a solução de gerenciamento de redes de computadores mais utilizada nas organizações, com estimativas de que 90% das grandes organizações do mundo utilizam-na para prover autenticação e autorização a ativos tecnológicos em seus negócios. A Microsoft, em seu relatório *Microsoft Digital Defense Report 2023*, registra que 43% dos clientes afetados por incidentes de segurança possuem configurações inseguras no *Active Directory* e há um bom custo-benefício quando essas configurações são revistas (melhora na segurança, alto impacto e facilidade de correção).

O que o TCU encontrou

43. A principal conclusão foi que, nas organizações auditadas, em todas as dimensões avaliadas, foram detectadas deficiências que geram riscos relevantes relacionados ao serviço de *Active Directory*, com destaque para as encontradas na dimensão de 'Configurações'.

44. O gráfico abaixo ilustra o grau de aderência às boas práticas das organizações auditadas:

[...]

45. O **escopo** da auditoria incluiu avaliar as seguintes dimensões:

45.1. A abordagem de proteção do AD-DS adotada pela organização, materializada em normativos e nos processos de gestão de pessoas, de capacitação em segurança e de documentação geral do ativo;

45.2. As configurações de arquitetura, gestão de grupo, acessos privilegiados, gestão de usuários e senhas, gestão de computadores, gestão de contas e serviço, gestão de contas de administrador local e processo periódico de identificação e tratamento de vulnerabilidades do AD-DS;

45.3. O monitoramento do AD-DS, consistindo na coleta de registros de auditoria (*logs*), da política de retenção de cópia de segurança de *logs* e do uso de ferramentas para monitoramento, análise e alerta de eventos;

45.4. Planos de contingência e recuperação do AD-DS, materializados em planos específicos documentados, na política de cópia de segurança e de testes de restauração.

46. A Figura 4 ilustra o modelo de avaliação utilizado na auditoria:

Figura 4 - Modelo de avaliação da gestão do serviço de domínios do *Active Directory*

[...]

Fonte: elaborada pela equipe de auditoria.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

47. Diante das deficiências que levaram à conclusão (parágrafo 43), o seguinte risco deve ser considerado pelas organizações, em especial aquelas com falhas graves nas configurações do AD-DS:

> 'Ataques cibernéticos combinados com falhas de configurações dos Serviços de Domínio *Active Directory* (AD-DS) poderão levar ao comprometimento dos domínios de rede, com consequente exfiltração, sequestro ou destruição de informações por meio de ataques de *ransomware*, o que poderá impactar negativamente a prestação de serviços públicos ao cidadão e a imagem da organização'.

48. Foi reforçada a necessidade de as organizações utilizarem uma abordagem que implementasse várias camadas de controles de segurança (defesa em profundidade), unindo esforços técnico e humano para que fosse criada uma barreira robusta e eficaz para proteção contra potenciais ataques.

Resultado

49. Diante dos resultados que lhes foram apresentados ao final da fiscalização (parágrafo 43), as três organizações auditadas enviaram à equipe Plano de Ação informando como pretendiam lidar com as deficiências que entenderam ser de maior risco. O envio desses planos evidenciou que a alta gestão dessas organizações assumiram a responsabilidade pelos riscos e pretendem melhorar a gestão de riscos no contexto dos Serviços de Domínio do *Active Directory* (AD-DS) da Microsoft.

Deliberação

50. As fiscalizações foram apreciadas por meio dos Acórdãos 750/2025-TCU-Plenário, 751/2025-TCU-Plenário e 752/2025-TCU-Plenário (todos do Rel. Min. Aroldo Cedraz).

3.5 F5: AUDITORIA EM GESTÃO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Objetivo da fiscalização

51. O **objetivo** da **F5** foi promover a melhoria no processo de Gestão de Resposta a Incidentes das organizações públicas por meio da avaliação dos controles administrativos e técnicos existentes. O TCU realizou duas auditorias de natureza operacional em duas organizações diferentes.

Por que o TCU fiscalizou

52. A relevância do *ransomware* no contexto nacional (parágrafo 12) é o ponto inicial de atenção ao tema. Dada sua importância, tem-se que o ataque de *ransomware* é um típico incidente de Segurança da Informação (SI), pois trata-se de evento que afeta a disponibilidade e confidencialidade dos ativos da organização, comprometendo severamente as operações da organização impactada.

53. A gestão de resposta a incidentes é um processo cujo objetivo é identificar, priorizar e tratar incidentes de SI – como um ataque de *ransomware* – com vista a restaurar a normalidade dos serviços e a conter os danos decorrentes. Ante a prevalência dos ataques de *ransomware*, aumenta a importância do processo de gestão de resposta a incidentes.

O que o TCU encontrou

54. A principal conclusão foi que, nas organizações auditadas, em todas as fases avaliadas foram detectadas deficiências que geram riscos relevantes relacionados à resposta de incidentes, expondo as organizações a riscos de SI que devem ser considerados.

55. O gráfico abaixo ilustra o grau de aderência às boas práticas das organizações auditadas:

[...]

56. O **escopo** da auditoria incluiu avaliar em qual medida os procedimentos executados nas quatro fases do processo de gestão de resposta a incidentes de segurança da informação estavam alinhados às boas práticas.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

57. De acordo com o documento técnico NIST 800-61r2/2012, o processo de resposta a incidentes é composto pelas seguintes fases, ilustrados na Figura 5 e detalhados em seguida.

Figura 5 - Ciclo de vida do processo de resposta a incidentes

[...]

Fonte: NIST *Special Publication* 800-61 *Revision 2* (2012), p. 21

57.1. **Preparação**: envolve atividades para garantir que os sistemas, redes e aplicações sejam suficientemente seguros e para que a organização esteja preparada para responder a incidentes.

57.2. **Detecção e Análise**: a detecção envolve atividades para monitorar sistemas, redes e *logs* para identificar atividades suspeitas que possam indicar um incidente, enquanto a análise envolve atividades para entender a causa, a fonte, os autores, as vulnerabilidades exploradas e o impacto do incidente nos negócios, sistemas e dados.

57.3. **Contenção, erradicação e recuperação**, que, em outros referenciais, são chamados de **tratamento**:

57.3.1. **Contenção**: envolve atividades para isolar os sistemas afetados e conter a propagação do incidente, como, por exemplo, desligar um sistema, desconectar da rede ou desabilitar uma de suas funcionalidades.

57.3.2. **Erradicação**: envolve atividades para remover a causa raiz do incidente, como, por exemplo, a remoção de *malware* e a desativação de contas de usuário violadas.

57.3.3. **Recuperação**: restauram-se os sistemas e os serviços afetados ao funcionamento normal.

57.4. **Pós-Incidente**: consiste em utilizar as lições aprendidas para entender o que aconteceu, como o incidente ocorreu e como evitar que ele se repita no futuro.

58. As deficiências que levaram à conclusão (parágrafo 54) estão listadas abaixo, com suas respectivas consequências:

58.1. Deficiências na preparação que levam ao **risco** de ineficácia ou intempestividade na resposta aos incidentes de segurança da informação, **com consequente** duração prolongada do incidente ou aumento do impacto adverso para a organização;

58.2. Deficiências na detecção e análise que levam ao **risco** de atraso ou não identificação de incidentes, **com consequente** diminuição das chances de sucesso das ações de tratamento (contenção, erradicação e recuperação);

58.3. Deficiências no tratamento que levam ao **risco** de atraso na tomada de decisão ou de baixa eficácia da ação escolhida durante a fase contenção, erradicação e recuperação, **com consequente** retardo no retorno dos sistemas/serviços afetados para os níveis operacionais normais ou recorrência de incidentes semelhantes; e

58.4. Deficiências no pós-incidente que levam ao **risco** de negligenciar oportunidades de melhoria no processo de gestão de resposta a incidentes de segurança da informação, **com consequente** ausência de validação e aprimoramento do plano de resposta a incidentes, das estratégias e dos procedimentos empregados, impactando negativamente na resiliência de SI de médio e longo prazo da organização.

Resultado

59. Diante dos resultados que lhes foram apresentados ao final da fiscalização (parágrafo 54), as duas organizações auditadas enviaram à equipe Plano de Ação informando como pretendiam lidar com as deficiências que entenderam ser de maior risco. O envio desses planos evidenciou que a alta gestão dessas organizações assumiram a responsabilidade pelos riscos e pretendem melhorar o seu processo de gestão de respostas a incidentes de SI.

Deliberação

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

60. As fiscalizações foram apreciadas por meio dos Acórdãos 509/2025-TCU-Plenário e 510/2025-TCU-Plenário (ambos do Rel. Min. Aroldo Cedraz).

3.6 F6: AUDITORIA DE GESTÃO DE CÓPIAS DE SEGURANÇA

Objetivo da fiscalização

61. O **objetivo** da **F6** foi promover a melhoria no processo de Gestão de Cópias de Segurança nas organizações públicas por meio da avaliação que abarcou aspectos como normativos instituídos, procedimentos de *backup*, segurança física e lógica do ambiente de *backup* e recursos disponíveis. O TCU realizou duas auditorias de natureza operacional em duas organizações diferentes.

Por que o TCU fiscalizou

62. A relevância do *ransomware* no contexto nacional (parágrafo 12) é o ponto inicial de atenção ao tema. Em um cenário em que o ataque de *ransomware* teve sucesso, ou seja, houve extração, encriptação ou destruição dos dados, as cópias de segurança são a principal medida para recuperar tais dados. Falhas ou negligências em *backups* podem resultar em perdas de dados críticas, afetando a resposta a crises e a confiança no governo.

O que o TCU encontrou

63. A principal conclusão foi que, nas organizações auditadas, em todas as dimensões avaliadas, foram detectadas deficiências relacionadas à gestão de cópias de segurança, expondo as organizações a riscos relevantes que devem ser considerados.

64. O gráfico abaixo ilustra o grau de aderência às boas práticas das organizações auditadas:

[...]

65. O escopo da auditoria incluiu avaliar a gestão de cópias de segurança e suas camadas de proteção em seis dimensões, conforme Figura 6, explanadas individualmente na sequência:

Figura 6 - Modelo de avaliação da gestão de cópia de segurança

[...]

Fonte: elaborada pela equipe de auditoria.

65.1. **Política de *backup*:** avalia os controles que envolvem a existência de norma interna que disciplina a gestão de cópia de segurança e se a organização auditada possui mecanismos para monitorar a implementação de tais determinações;

65.2. **Planos e procedimentos:** avalia o conjunto de práticas, efetivamente implementadas, para o bom funcionamento da gestão de cópias de segurança;

65.3. **Segurança física:** avalia o conjunto de controles de segurança física do ambiente de processamento e armazenamento de cópias de segurança. Incluem-se, por exemplo, nessa avaliação o controle de umidade e temperatura, proteção contra incêndio e controle de acesso físico;

65.4. **Segurança lógica:** avalia o conjunto de controles de segurança lógica implementados para proteger o ambiente de processamento e armazenamento de cópias de segurança. Incluem-se, por exemplo, nessa avaliação o controle de acesso lógico, criptografia dos dados e uso de ferramentas contra códigos maliciosos *(antimalware)*;

65.5. **Testes de restauração**: avalia a realização dos testes de restauração das cópias de segurança.

65.6. **Recursos disponíveis**: avalia os recursos disponíveis para a realização da gestão de cópias de segurança, incluem-se nessa avaliação os recursos de pessoas (força de trabalho), capacitação, infraestrutura (física e tecnológica) e processos. Este eixo de avaliação foi executado para contextualizar as demais avaliações e fornecer elementos para avaliação das causas das deficiências encontradas.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

66. As deficiências que levaram à conclusão (parágrafo 63) expõem as organizações ao seguinte risco:

> 'A ocorrência de ataques de *ransomware* na organização c/c deficiências na gestão de cópias de segurança **podem levar ao** comprometimento da confidencialidade, da integridade e da disponibilidade dos dados contidos nas cópias de segurança **com consequente** impacto negativo na recuperação de dados eventualmente perdidos (tempo de recuperação e perda de dados inaceitáveis para as áreas de negócio e clientes)'

67. Foram encontradas deficiências em todas as dimensões avaliadas no conjunto de organizações auditadas. Foi reforçada a necessidade de as organizações utilizarem uma abordagem que implementasse várias camadas de controles de segurança (defesa em profundidade), unindo esforços técnico e humano para que fosse criada uma barreira robusta e eficaz para proteção de seu último recurso de continuidade de negócio, que é o *backup*.

Resultado

68. Diante dos resultados que lhes foram apresentados ao final da fiscalização (parágrafo 63), as duas organizações auditadas enviaram à equipe Plano de Ação informando como pretendiam lidar com as deficiências que entenderam ser de maior risco. O envio desses planos evidenciou que a alta gestão dessas organizações assumiram a responsabilidade pelos riscos e pretendem melhorar o seu processo de gestão de cópias de segurança.

Deliberação

69. As fiscalizações foram apreciadas por meio dos Acórdãos 537/2025-TCU-Plenário e 639/2025-TCU-Plenário (ambos do Rel. Min. Aroldo Cedraz).

4 ESTRATÉGIA DE MULTIPLICAÇÃO DOS RESULTADOS

70. A estratégia adotada pela AudTI para multiplicação dos resultados foi semelhante para todos os trabalhos que compõem esse consolidador e foi composta pelas seguintes iniciativas:

70.1. Elaboração de guias sobre o tema da auditoria, com foco em dar suporte à tomada de decisão dos gestores sobre a implementação dos controles avaliados a partir de uma abordagem baseada em risco;

70.2. Disponibilização dos Questionários de Avaliação de Controles Internos (QACI) utilizados nas auditorias no portal do TCU (https://tcu.gov.br/dasi); e

70.3. Realização de eventos (*workshops*) no YouTube para apresentar e debates os temas das auditorias.

71. Para a F1, foi elaborado o guia 'Matriz de Riscos e Controles para serviços de hospedagem Web, e-mail e DNS', que apresenta a descrição dos tipos de ataque que podem ser executados em caso de erros de configurações dos controles, de forma a introduzir os gestores, que estão nas defesas das organizações públicas, ao mundo das táticas, das técnicas e dos procedimentos (TTP) utilizados pelos agentes de ameaça no mundo cibernético. Para apoiar a gestão de riscos, são indicados exemplos de referências com detalhes técnicos de como implementar os controles. O documento inclui, ainda, uma estimativa preliminar de custos e benefícios relacionados à implementação de cada controle. O guia está publicado no site https://tcu.gov.br/dasi.

72. Para a F4, está em fase final de elaboração o guia 'Matriz de Riscos e Controles para o serviço de domínio *Microsoft Active Directory*', que fará uma abordagem abrangente sobre riscos e controles no âmbito dessa ferramenta. O documento visa apoiar as organizações públicas e privadas na gestão de riscos relacionados ao AD-DS. Para cada dimensão de avaliação, o guia traz os controles, testes para verificar sua existência/implementação no ambiente, riscos da não implementação de cada controle, critérios, custo e benefício estimados por controle.

73. Os QACI que estão disponibilizados no site https://tcu.gov.br/dasi são uma adaptação dos papéis de trabalho utilizados nas auditorias para avaliar a aderência às boas práticas dos controles aplicáveis ao tema de cada fiscalização. A versão publicada visa

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

apoiar organizações públicas e privadas na gestão de riscos em cada um dos temas auditados ao permitir que realizem avaliação interna dos seus controles, identificando as lacunas e produzindo um plano de ação para lidar com tais riscos.

74. Os *workshops* são chamados de Protege-TI Online e são eventos ao vivo realizados no canal no Tribunal de Contas da União no YouTube. Os seis eventos estão elencados na lista de reprodução 'Protege-TI Online' acessível no seguinte link: https://www.youtube.com/@TCUoficial/playlists. Além de acompanhar o evento ao vivo, os participantes poderiam se inscrever no *workshop* no portal do Instituto Serzedello Corrêa (ISC) para participar de fórum de discussões, realizar atividades e ganhar certificado de conclusão dos cursos.

75. A exceção da F1, as demais fiscalizações do Protege-TI 23/24 foram sigilosas em decorrência do tema (segurança da informação). Devido à importância dos temas avaliados, pensou-se nesses *workshops* como uma forma de disseminar o conhecimento produzido nas auditorias de forma anonimizada, sem divulgar detalhes das fiscalizações, mas compartilhando os principais riscos e controles de cada tema.

76. Dessa forma, o principal objetivo desses eventos era disseminar para o público geral a importância de cada um dos temas que foram auditados, a partir das experiências dos auditores e do *feedback* dos auditados, bem como divulgar os guias e QACIs disponibilizados para que os gestores das mais variadas organizações pudessem se valer desses artefatos para aprimorar sua gestão de risco em SI.

5 DAS CAUSAS-RAIZ

77. As auditorias que compuseram o Protege-TI 23/24 evidenciaram diversos achados e suas causas. Como a abordagem foi a de avaliação por meio de QACI, que contemplavam controles em cada dimensão, muitas das causas também foram identificadas como achados.

78. Utilize-se como exemplos dois grupos de achados, um relacionado à F2 e outro relacionado à F4:

78.1. F2: para o **achado A** 'X usuários clicaram em link malicioso durante simulação de *phishing* realizada na auditoria', tem-se como causa 'a organização não possui um programa de conscientização dos usuários em ataques cibernéticos de engenharia social'. Tal causa foi identificada na auditoria como **achado B**;

78.2. F4: para o **achado C** 'existem Y contas ativas no grupo *Domain Admin* do AD da organização, quando só deveria haver uma', tem-se como causa 'a organização não possui um processo estabelecido de identificação, análise e correção de falhas nas configurações do AD'. Tal causa foi identificada na auditoria como **achado D**.

79. Tudo que estava contemplado em QACI foi identificado como achado, mesmo que o fato viesse a ser, também, causa de outro achado. Assim, as auditorias se aprofundaram nas causas até certo nível, conforme o escopo da auditoria.

80. No entanto, as fiscalizações buscaram **levantar** um conjunto de possíveis causas-raiz, ou seja, aquelas que estariam dificultando ou impedindo o tratamento das causas evidenciadas. Nos exemplos citados, seriam perguntas como '...e por que não há programa de conscientização do usuário?' ou '...e por que não há processo de gestão de falhas de configuração do AD estabelecido?'.

81. Ressalte-se que esse levantamento ocorreu após a apresentação dos achados, em entrevista com os gestores responsáveis, e não foi suportado por testes de auditoria posteriores. Ou seja, não há evidências além do próprio relato dos gestores que suportem essas causas-raiz levantadas. Essas causas-raiz não foram rotuladas como achados justamente devido a essa ausência de evidências. O conjunto de causas-raiz relatadas, por fiscalização, encontra-se no (...)

82. De forma gráfica, para o exemplo citado, teríamos:

[...]

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

83. Isto posto, a **falta de pessoal capacitado** foi a causa-raiz comum, relatada pelos gestores de todas as organizações auditadas, quando questionados possíveis fatores que contribuíram para as causas evidenciadas.

84. A falta de pessoal na área de TI não é novidade. O TCU já evidenciou que essa escassez em uma realidade da administração pública federal por meio dos Acórdãos 1.200/2014-TCU-Plenário (Rel. Min. Raimundo Carreiro) e 2.326/2017-TCU-Plenário (Rel. Min. Aroldo Cedraz), deliberações que estão sendo monitoradas no TC 007.353/2024-3. O tema das fiscalizações do Protege-TI 23/24 é segurança da informação, que possui elevado grau de interconexão com o tema TI. Falta de pessoal capacitado em SI não é, portanto, um fato inesperado, e deve ser endereçado pelos órgãos governantes superiores do setor público federal.

85. Por outro lado, são diversos os fatores que levam à escassez de pessoal em uma determinada área e a solução para esse problema não é simples. Levando em conta essa complexidade, o fato de que não fez parte do escopo dos trabalhos do Protege-TI analisar os fatores que levam à falta de pessoal suficiente e capacitado em SI na administração pública federal e a ausência de evidências nos autos para as causas levantadas, não será proposta recomendação específica para essa causa-raiz comum no âmbito deste processo.

86. Ademais, como é um problema que já vem sendo acompanhado pela AudTI em outra ação de controle (parágrafo 84), entende-se ser lá o espaço apropriado para proposição de eventuais soluções.

87. Por fim, é importante frisar que as causas evidenciadas, que figuraram como achados nas auditorias, fizeram todas parte dos planos de ação apresentados pela alta administração dos auditados, que se comprometeram a tomar medidas para mitigar os riscos que tais achados representam.

6. AVALIAÇÃO DOS GESTORES

88. Ao final de cada fiscalização, as equipes de auditoria enviam um questionário de avaliação da fiscalização aos gestores. O objetivo é conhecer a **opinião da alta administração** sobre os resultados alcançados e a forma de condução dos trabalhos, aprimorando, dessa forma, a qualidade dos trabalhos de fiscalização. O questionário possui questões sobre os resultados alcançados após a realização das fiscalizações e sobre a forma de condução dos trabalhos.

89. Os gestores avaliaram as auditorias a partir da seguinte tabela:

[...]

90. Na pergunta final, que sintetiza a satisfação dos gestores com a fiscalização ('Qual o seu grau de satisfação com esta fiscalização?'), nove responderam que estavam totalmente satisfeitas (nota 10), e apenas uma organização avaliou item como 9.

91. Sobre o resultado das fiscalizações para as organizações auditadas:

91.1. 83% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'Após a fiscalização, **temos mais clareza quanto ao nível atual de risco** associado ao tema da auditoria', enquanto 17% marcaram a opção '*Concordo mais do que discordo*';

91.2. 83% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'A interação com equipe do TCU, incluindo a apresentação da avaliação preliminar antes da chegada do acórdão, **contribuiu para melhorar a gestão dos riscos** associado ao tema da auditoria', enquanto 17% marcaram a opção '*Concordo mais do que discordo*'.

91.3. 100% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'Hoje a organização tem um **plano de ação** para aumentar sua resiliência aos ataques direcionados ao tema da auditoria'.

91.4. 100% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'A avaliação preliminar da equipe do TCU **contribuiu** para a elaboração do plano de ação acima mencionado'.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

91.5. 100% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'A **autoridade máxima da organização tem conhecimento** do mencionado plano de ação'.

91.6. 100% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'Nas **reuniões iniciais** (reunião técnica e de apresentação para a Alta Administração), a **equipe de fiscalização do TCU apresentou os principais elementos e diretrizes do trabalho** que seria executado'.

91.7. 100% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'Ao longo da fiscalização, os **elementos e diretrizes acima foram seguidos** pela equipe do TCU durante a execução do trabalho'.

91.8. 66% das organizações marcaram a opção '*Concordo totalmente*' para a seguinte pergunta: 'Os trabalhos da equipe de fiscalização **não interferiam ou interferiram de forma aceitável** na rotina de trabalho da organização', enquanto 17% marcaram a opção '*Concordo mais do que discordo*' e 17% marcaram a opção '*Discordo mais do que concordo*'.

92. A auditoria F1 testou 14.000 domínios em milhares de organizações, não sendo viável o envio do questionário. No entanto, no voto condutor do acórdão resultante da F1, o relator destacou o caráter inovador do trabalho, que se utilizou de técnicas e ferramentas de segurança ofensiva para analisar as configurações de serviços que são utilizados por toda e qualquer organização, pública ou privada, que mantenha algum grau de presença na internet: a hospedagem e publicação de *sites*, os servidores de e-mail e a infraestrutura que realiza a tradução de nomes como www.tcu.gov.br para os endereços IP utilizados para comunicação na rede mundial.

93. Abaixo alguns comentários realizados pelos gestores sobre as fiscalizações realizadas no âmbito do Protege-TI:

> 'O trabalho desempenhado pela equipe do TCU foi excelente, pois contribuiu para nosso amadurecimento nas questões relativas ao backup e processos de negócio para procedimentos de recuperação de desastres ou ataques de *ransomware*. Julgamos muito importante o trabalho que está sendo conduzido, pois aumentará o grau de resiliência dos órgãos quanto aos desafios de segurança de dados públicos digitais frente aos diversos ataques *hackers* que tem acontecido nos últimos anos.
>
> Essa nova proposta do Tribunal de Contas da União (TCU), que traz especialistas em determinadas ferramentas e processos críticos do órgão auditado, é verdadeiramente revolucionária. Nesse modelo, a identificação de vulnerabilidades e a apresentação de diversas melhores práticas não apenas auxiliam diretamente o órgão auditado, mas também demonstram que o TCU não é apenas um órgão fiscalizador, mas um parceiro com o qual podemos contar. Gostaria de expressar minha gratidão à equipe técnica do TCU, que foi extremamente compreensiva diante das dificuldades que enfrentamos. Sua abordagem educativa e paciência ao considerar nossas limitações foram notáveis. Deixo registrado meu 'Aceite' para qualquer novo convite relacionado a esse inovador modelo de auditoria. Parabenizo aqueles que pensaram 'fora da caixa' e criaram um processo de auditoria mais assertivo e colaborativo.
>
> Consideramos essa auditoria extremamente enriquecedora, agregando muito conhecimento e aprimorando às ações de segurança. A auditoria foi focada e técnica, embasada em ferramentas e *frameworks* reconhecidos internacionalmente. Gostamos muito da abordagem utilizada pelo TCU nos trabalhos dessa auditoria. Foi notória a qualidade técnica dos auditores, bem como o quanto ela agregou valor para a segurança do AD da nossa organização'.

7 CONCLUSÃO

94. A partir do conjunto de organizações auditadas nas fiscalizações que compuseram o Protege-TI 23/24, é possível afirmar que foram encontradas **deficiências de SI em todos os grupos, dimensões ou fases avaliadas nas auditorias** (parágrafos 25, 33, 43, 54 e 63).

95. Essa situação encontrada demonstra um quadro de **exposição a riscos de SI** das organizações fiscalizadas, que foram assumidos pela alta administração de cada organização

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

auditada, que os incorporaram à sua gestão de riscos a partir de um plano de ação (parágrafos 28, 39, 49, 59 e 68).

96. Embora o rol de auditados nas fiscalizações do Protege-TI 23/24 não represente uma amostra estatística da realidade da administração pública federal, este aponta para um indício do nível de maturidade das organizações federais como um todo. Indício esse que ganha força a partir do resultado da auditoria operacional realizada nos controles de cibersegurança das organizações do Sistema de Administração dos Recursos de Tecnologia da Informação – Sisp (Acórdão 2.387/2024-TCU-Plenário, Rel. Min. Augusto Nardes), que concluiu que 'as organizações do Sisp estão aquém do esperado no que se refere à implementação de medidas de segurança cibernética' (TC 010.390/2024-3, peça 200, p. 3).

97. Ao analisar as **causas-raiz** dos achados levantadas junto aos gestores, percebe-se que todas as fiscalizações apontaram para a **falta de pessoal capacitado**, que pode ser entendida como causa comum das deficiências de todos os objetos que foram auditados no Protege-TI 23/24 e que já havia sido identificada em fiscalização anterior do TCU (seção 5).

98. O **valor gerado** a partir das fiscalizações do Protege-TI 23/24 pode ser visto sob a perspectiva interna à auditoria – para os auditados – e externa, para toda a sociedade:

98.1. Para as organizações auditadas:

98.1.1. Houve uma melhoria evidenciada na sua gestão de riscos de SI, visto que todas apresentaram plano de ação para tratar os riscos identificados nas fiscalizações (parágrafo 95), resultando no aprimoramento na identificação dos riscos (que estão listados no plano de ação) e no aumento da participação da alta administração, ao assumir o seu papel de responsável pelo tratamento dos riscos de SI (ao aprovar o plano);

98.1.2. Há também uma melhoria potencial na gestão de riscos, a depender do grau de implementação dos planos de ação produzidos pelas organizações.

98.2. Para os gestores de TI e SI de organizações públicas e privadas, essas fiscalizações foram o principal insumo para os *workshops* online realizados no YouTube (parágrafos **Error! Reference source not found., Error! Reference source not found., Error! Reference source not found., Error! Reference source not found. e Error! Reference source not found.**) com amplo público-alvo e de alcance nacional.

99. Dessa forma, entende-se que as fiscalizações do Protege-TI 23/24, individualmente, cumpriram seus objetivos de promover a melhoria na gestão de riscos de SI das auditadas em seus respectivos objetos (parágrafos 23, 31, 41, 51 e 61), assim como o primeiro ciclo da **estratégia** Protege-TI também foi bem sucedido, visto que contribuiu – a partir de seus valores gerados interna e externamente (parágrafo 98) – para 'tornar seguro o ambiente digital sob a governabilidade do Brasil' (parágrafo 1).

8 PROPOSTA DE ENCAMINHAMENTO

100. Ante o exposto, submetem-se os autos ao gabinete do Relator, Ministro Aroldo Cedraz, com as seguintes propostas:

100.1. Enviar cópia do relatório, voto e acórdão que vierem a ser proferidos, bem como desta instrução, à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) ao Conselho Nacional de Justiça (CNJ), ao Conselho Nacional do Ministério Público (CNMP), à Câmara dos Deputados e ao Senado Federal;

100.2. Autorizar a Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI) a divulgar as informações constantes das ações de controles consolidadas neste acompanhamento, por meio de ficha-síntese, palestras e eventos;

100.3. Arquivar os presentes autos com fundamento no art. 169, V, do Regimento Interno do TCU".

É o relatório.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982493.

VOTO

Em exame, relatório de acompanhamento que busca consolidar os resultados das auditorias operacionais no âmbito do primeiro ciclo do projeto "PROTEGE-TI", realizadas ao longo dos exercícios 2023 e 2024, em organizações da administração pública federal.

2. O PROTEGE-TI é a estratégia de controle externo da Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI) em segurança da informação e proteção de dados, com o propósito de "tornar seguro o ambiente digital sob a governabilidade do Brasil". A iniciativa integra um conjunto de até seis ações de controle voltadas para induzir a adoção de boas práticas e o cumprimento de normas referentes ao tema por parte da administração pública federal, com destaque para a avaliação de riscos e controles técnicos de segurança cibernética e da informação.

3. Conforme esclarecido pela AudTI, trata-se de estratégia ágil, executada em ciclos anuais orientados pela priorização de objetos classificados por categorias de riscos.

4. As categorias de riscos englobam os riscos estratégicos, como a atual situação da política nacional de cibersegurança; os riscos táticos, como o nível de maturidade em cibersegurança das organizações do poder executivo federal; e os riscos operacionais, decorrentes da insuficiência de controles técnicos que protejam as organizações dos principais vetores de ataques cibernéticos, como aqueles utilizados nos ataques ao Superior Tribunal de Justiça (STJ) em 2020 e que impactaram negativamente o andamento dos processos durante alguns meses.

5. O ciclo atual em exame teve como foco a redução de riscos operacionais no caminho de ataque de *ransomware*[1] e englobou aspectos relacionados ao acesso inicial, à gestão de incidentes, às configurações do ambiente computacional e aos procedimentos para realização e restauração de cópias de segurança de ambientes críticos.

6. A AudTI definiu as fiscalizações individuais a partir dos seguintes objetos: a) suscetibilidade a ataques de *phishing*; b) configurações de serviços *web*, *e-mail* e DNS; c) gestão de controle de acesso e credenciais; d) vulnerabilidades no serviço de *Active Directory*; e) cópias de segurança ou *backup*; e f) gestão de incidentes.

7. O objetivo das ações permitiu gerar informações capazes de contribuir para a evolução da segurança cibernética da administração pública federal. Além disso, também foi possível avaliar se as medidas adotadas pelos entes auditados são adequadas para enfrentar as ameaças crescentes de ataques no ambiente virtual.

8. Como destacado, o elemento direcionador do PROTEGE-TI neste ciclo consistiu na prevenção de ataques de *ransomware,* os quais constituem a maior parcela das ameaças oriundas da internet à segurança das organizações brasileiras. Segundo estudos de empresas especializadas no tema, o Brasil foi o segundo país com maior número de ofensivas desse tipo em 2022.

9. Segundo o relatório do acompanhamento, a ação de controle consistiu, inicialmente, em seis fiscalizações, detalhadas a seguir, com os respectivos objetivos, deliberações e conclusões.

10. Auditoria dos controles de segurança dos servidores *web, e-mail* e DNS (*Domain Name System*) – (F1): promover a melhoria na gestão de riscos dos vetores de ataque referentes à exploração de vulnerabilidades e falhas de configuração de serviços expostos à internet e à realização de ataques de *phishing*[2] para obtenção de credenciais ou acessos a sistemas. Foi exarado

---

[1] *Ransomware* é um tipo de *malware* (*software* malicioso) que sequestra os dados de um sistema ou dispositivo, criptografando-os e exigindo um resgate (do inglês, *ransom*) para descriptografar e restaurar o acesso aos dados.

2 Forma específica de ataque de engenharia social. Tática utilizada por cibercriminosos (atacantes) para manipular a

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982495.

o acórdão 523/2024 - Plenário[3], que corresponde à única fiscalização não sigilosa no âmbito do Protege-TI 23/24.

10.1. Na auditoria, foram testados milhares de domínios de organizações públicas dos três poderes da União e das três esferas de governo, a fim de identificar se existem falhas de configuração em servidores *web, e-mail e DNS (Domain Name Service)* acessíveis pela internet e que podem ser exploradas por agentes de ameaça.

10.2. A ação de controle identificou sete riscos e apontou que pode ocorrer a manipulação de tráfego de rede, comprometimento de contas de usuários, roubo, vazamento e perda de dados ou mesmo disrupção dos sistemas de organizações públicas.

10.3. As conclusões e resultados da fiscalização foram comunicados a oito organizações, que representam a multiplicidade de organizações detentoras dos domínios avaliados, para que avaliem a adoção de medidas e a elaboração de estratégias para orientar as organizações que se encontram na sua área de atuação sobre a gestão dos riscos decorrentes da não implantação dos controles analisados.

11. Auditoria sobre o vetor de ataque *phishing* – (F2): promover a melhoria da gestão de riscos nas organizações públicas no contexto do vetor de ataque *phishing* por meio da avaliação de controles administrativos, técnicos e de conscientização em relação às boas práticas sobre o tema. Este Tribunal realizou três auditorias de natureza operacional em três organizações diferentes e foram exarados os acórdãos 2079/2024-Plenário, 2080/2024-Plenário e 2081/2024-Plenário[4].

11.1. Como principal conclusão, a unidade especializada registrou que existe suscetibilidade dos usuários das organizações a contribuírem, ainda que não intencionalmente, com ataques de *phishing*. Além disso, foram detectadas, nos eixos avaliados (administrativo e técnico), deficiências ou oportunidades de melhoria que geram riscos relevantes relacionados ao vetor de ataque *phishing*.

11.2. Em face dos resultados apresentados ao final da fiscalização, as três organizações auditadas enviaram à equipe um plano de ação informando como pretendiam lidar com as deficiências classificadas como de maior risco. O envio desses planos evidenciou que a alta gestão dessas organizações assumiu a responsabilidade pelos riscos e pretende melhorar a gestão de risco no contexto do vetor de ataque *phishing*.

12. Auditoria de gestão de controle de acesso e credenciais – (F3): promover a melhoria na gestão de riscos de segurança da informação nas organizações públicas no contexto dos Serviços de Domínio do *Active Directory* (AD-DS) da *Microsoft*, por meio da avaliação dos controles administrativos e técnicos existentes. O Tribunal realizou três auditorias de natureza operacional em três organizações diferentes.

12.1. A AudTI optou por terminar o acompanhamento sem a realização da F3. A unidade especializada esclareceu que o tema foi abordado em duas fiscalizações: inspeção do Siafi [5] e auditoria do portal gov.br[6].

13. Auditoria de gestão serviços de domínio do *Active Directory* - (F4): promover a melhoria na gestão de riscos de segurança da informação nas organizações públicas no contexto dos serviços de domínio do *Active Directory* (AD-DS) da *Microsoft*, por meio da avaliação dos controles administrativos e técnicos existentes. Esta Corte realizou três auditorias de natureza

---

psicologia humana e induzir indivíduos a realizarem ações que comprometam a segurança ou divulguem informações sensíveis.

3 Relator ministro Aroldo Cedraz.

4 Todos da relatoria do ministro Aroldo Cedraz.

5 TC 024.560/2024-3, relator ministro Bruno Dantas.

6 TC 015.635/2025-2, relator ministro Aroldo Cedraz.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982495.

operacional em três organizações diferentes, tendo sido exarados os acórdãos 750/2025-Plenário, 751/2025-Plenário e 752/2025-Plenário[7].

13.1. A unidade especializada detectou deficiências nas organizações auditadas, em todas as dimensões avaliadas, com riscos relevantes relacionados ao serviço de *Active Directory*, com destaque para a deficiência na dimensão de "configurações".

13.2. O escopo da ação de controle incluiu avaliar as dimensões relativas à abordagem de proteção AD-DS da organização, configurações de arquitetura, gestão de grupo, acessos privilegiados, gestão de usuários e senhas, gestão de computadores, gestão de contas e serviço, gestão de contas de administrador local e processo periódico de identificação e tratamento de vulnerabilidades do AD-DS, planos de contingência e recuperação do AD-DS, dentre outras.

13.3. Ao fim, a unidade especializada registrou a necessidade de as organizações utilizarem uma abordagem que implementasse várias camadas de controles de segurança (defesa em profundidade), unindo esforços técnico e humano para criar uma barreira robusta e eficaz de proteção contra potenciais ataques.

14. Auditoria em gestão de resposta a incidentes de segurança da informação – (F5): promover a melhoria no processo de gestão de resposta a incidentes das organizações públicas por meio da avaliação dos controles administrativos e técnicos existentes. Foram realizadas duas auditorias de natureza operacional em duas organizações diferentes, tendo sido exarados os acórdãos 509/2025-Plenário e 510/2025-Plenário[8].

14.1. A unidade especializada detectou deficiências, nas organizações auditadas, em todas as fases avaliadas, gerando riscos relevantes relacionados à resposta de incidentes e expondo as organizações a riscos de segurança da informação.

14.2. Em face dos resultados apresentados, as duas organizações auditadas enviaram plano de ação informando como pretendiam lidar com as deficiências de maior risco. O envio dos planos evidenciou que a alta gestão das organizações assumiu a responsabilidade pelos riscos e indicou que pretende melhorar o seu processo de gestão de respostas a incidentes.

15. Auditoria de gestão de cópias de segurança – (F6): promover a melhoria no processo de gestão de cópias de segurança nas organizações públicas por meio da avaliação que abarcou aspectos como: normativos instituídos, procedimentos de *backup*, segurança física e lógica do ambiente de *backup* e recursos disponíveis. O Tribunal realizou duas auditorias de natureza operacional em duas organizações diferentes e foram exarados os acórdãos 537/2025-Plenário e 639/2025-Plenário[9].

15.1. O escopo da auditoria incluiu avaliar a gestão de cópias de segurança e suas camadas de proteção em seis dimensões: política de *backup*, planos e procedimentos, segurança física, segurança lógica, testes de restauração e recursos disponíveis.

15.2. Foram encontradas deficiências em todas as dimensões avaliadas e foi reforçada a necessidade de as organizações utilizarem uma abordagem que implementasse várias camadas de controles de segurança (defesa em profundidade), unindo esforços técnico e humano para que fosse criada uma barreira robusta e eficaz para proteção de seu último recurso de continuidade de negócio, que é o *backup*.

16. Ao fim da consolidação das auditorias, a AudTI apresentou a estratégia adotada para a multiplicação dos resultados, composta, em resumo, pelas seguintes iniciativas: a) elaboração de

7 Todos da relatoria do ministro Aroldo Cedraz.

8 Todos da relatoria do ministro Aroldo Cedraz.

9 Todos da relatoria do ministro Aroldo Cedraz.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982495.

guias sobre o tema das auditorias, com foco em dar suporte à tomada de decisão dos gestores sobre a implementação dos controles avaliados a partir de uma abordagem baseada em risco; b) disponibilização dos questionários de avaliação de controles internos[10] utilizados nas auditorias no portal do Tribunal[11]; c) realização de eventos, como workshops no *youtube* para apresentação e debates e; d) elaboração de matrizes de riscos e controles.

17. A unidade instrutiva esclareceu também que, ao final de cada fiscalização, as equipes de auditoria enviam um questionário de avaliação da fiscalização aos gestores com o objetivo de conhecer a opinião da alta administração sobre os resultados alcançados e a forma de condução dos trabalhos, de modo a aprimorar a qualidade das ações de controle.

18. Verifico que a estratégia de multiplicação de resultados pode assegurar maior abrangência quanto ao impacto dos trabalhos realizados, para além das organizações auditadas, possibilitando induzir um processo de maturação com a difusão de informações sobre o tema para públicos-alvo, tendo como base deliberações em processos de controle externo sobre segurança da informação e boas práticas nacionais e internacionais, ampliando o alcance da atuação pedagógica desta Corte e permitindo uma evolução mais rápida da gestão da segurança cibernética e da informação em âmbito nacional.

19. Por fim, consoante destacado no relatório, para que uma organização esteja preparada para prevenir e responder a ataques é essencial que disponha de normas, processos e procedimentos bem definidos, além de soluções tecnológicas (*hardware, software* e serviços) que resultem na implementação de controles eficazes para tratamento dos riscos cibernéticos.

Ante o exposto, manifestando concordância com o relatório e a proposta de encaminhamento, voto para que o Tribunal adote a minuta de deliberação que ora submeto à apreciação deste Colegiado.

TCU, Sala das Sessões, em 21 de outubro de 2026.

ODAIR CUNHA
Relator

10 QACI.

11 https://tcu.gov.br/dasi.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80982495.

ACÓRDÃO Nº 2923/2026 – TCU – Plenário

1. Processo nº TC 017.092/2023-0.
2. Grupo I – Classe de Assunto: V – Relatório de Acompanhamento.
3. Interessado: Tribunal de Contas da União.
4. Órgão: Tribunal de Contas da União.
5. Relator: Ministro Odair Cunha.
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:

VISTO, relatado e discutido este relatório de acompanhamento que teve como objetivo consolidar os resultados das auditorias operacionais de segurança da informação e segurança cibernética em organizações da administração pública federal, em atendimento ao acórdão 1104/2023 – Plenário.

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. enviar cópia da instrução de peça 7, do relatório, do voto e do acórdão, à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) ao Conselho Nacional de Justiça (CNJ), ao Conselho Nacional do Ministério Público (CNMP), à Câmara dos Deputados e ao Senado Federal;

9.2. autorizar a Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI) a divulgar as informações constantes das ações de controle consolidadas no acompanhamento, por meio de ficha-síntese, palestras e eventos;

9.3. arquivar o processo, com fundamento no art. 169, V, do Regimento Interno.

10. Ata n° 41/2026 – Plenário.
11. Data da Sessão: 21/10/2026 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-2923-41/26-P.
13. Especificação do quórum:
13.1. Ministros presentes: Walton Alencar Rodrigues (na Presidência), Benjamin Zymler, Jhonatan de Jesus, Odair Cunha (Relator) e Rodrigo Pacheco.
13.2. Ministros-Substitutos convocados: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e Weder de Oliveira.
13.3. Presidente não votou (Resolução-TCU 375/2025, art. 3º).

(Assinado Eletronicamente)
WALTON ALENCAR RODRIGUES
na Presidência

(Assinado Eletronicamente)
ODAIR CUNHA
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 80982498.