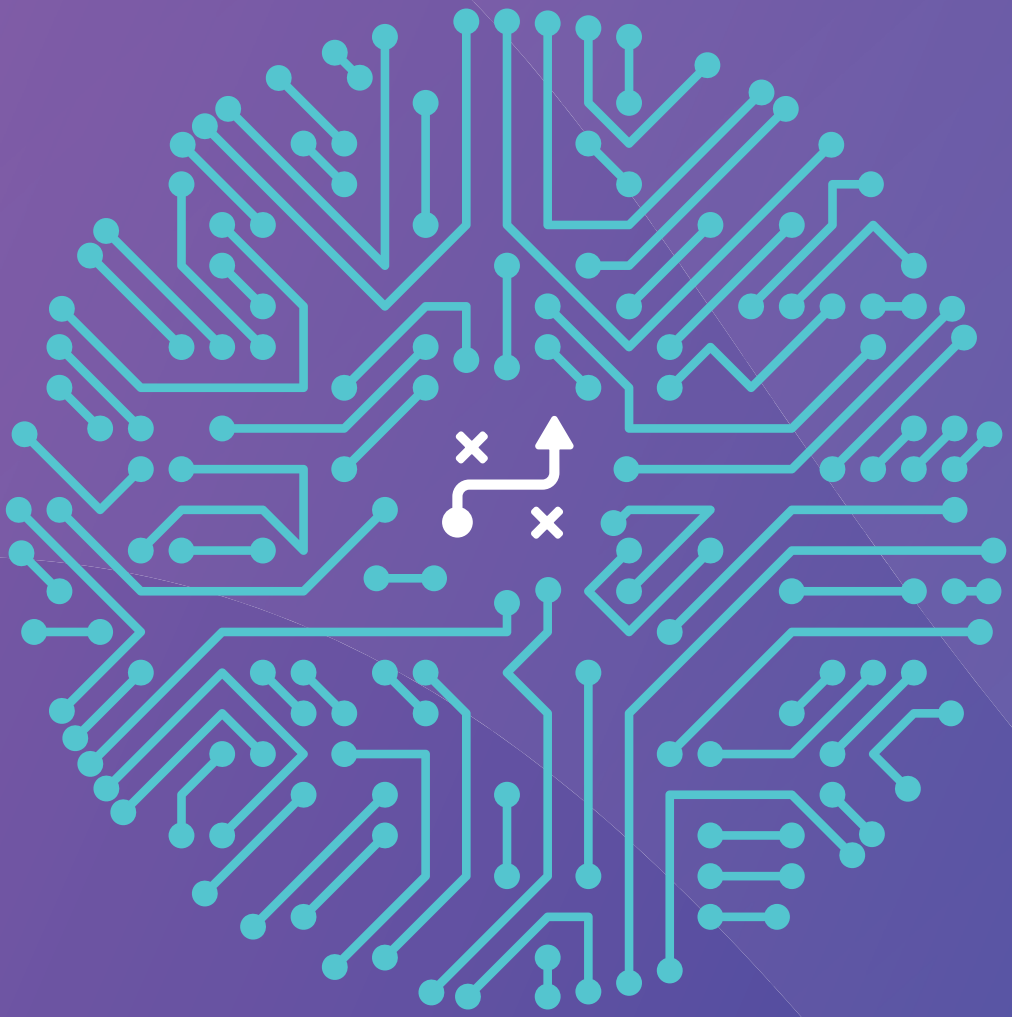
TRIBUNAL DE CONTAS DA UNIÃO

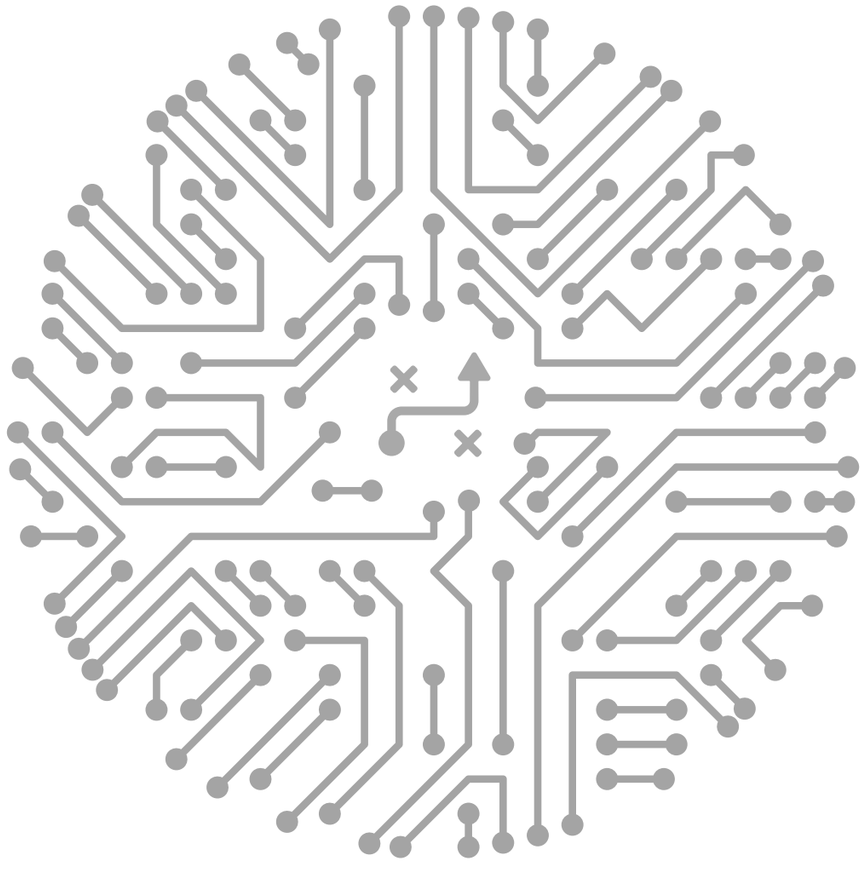


ESTRATÉGIA DE FISCALIZAÇÃO DO TCU EM SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

2020-2023

REPÚBLICA FEDERATIVA DO BRASIL
TRIBUNAL DE CONTAS DA UNIÃO

TRIBUNAL DE CONTAS DA UNIÃO



ESTRATÉGIA DE FISCALIZAÇÃO DO TCU EM SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

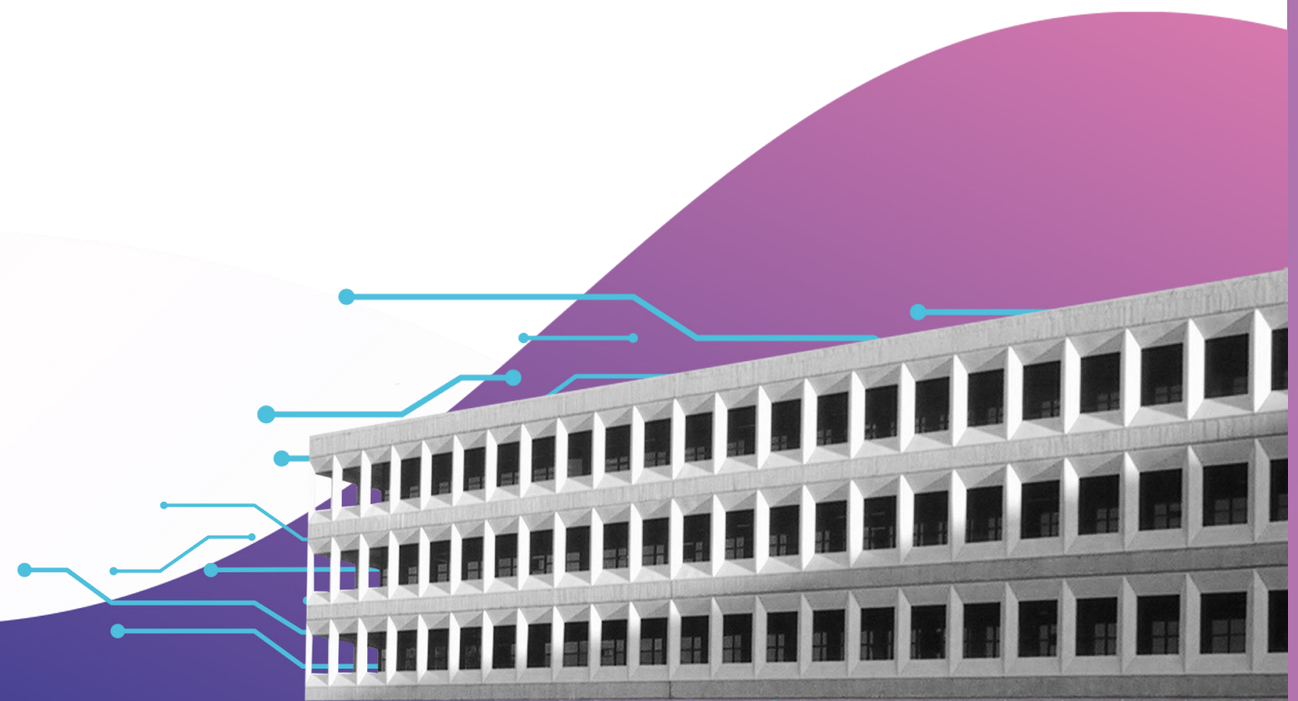
2020-2023

BRASÍLIA, 2021.

Brasil. Tribunal de Contas da União.

Estratégia de Fiscalização do TCU em segurança da informação e segurança cibernética 2020-2023

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa



SUMÁRIO

1 CONTEXTUALIZAÇÃO

Com a digitalização dos serviços públicos, vulnerabilidades e falhas de segurança da informação (SegInfo) em sistemas relevantes podem afetar significativamente o governo e os cidadãos, tornando-se imprescindível, então, assegurar a disponibilidade, integridade, confiabilidade e autenticidade das informações que viabilizam a transformação digital (TD) desses serviços.

São vários os riscos decorrentes de falhas na gestão da SegInfo, entre eles a perda de integridade de dados públicos e pessoais, a indisponibilidade de serviços públicos, o vazamento de informações sigilosas, a invasão da privacidade do cidadão e, inclusive, vultosas perdas financeiras. Em um contexto de TD, com cada vez mais informações e serviços públicos disponíveis na internet, aumentam os riscos à segurança das informações decorrentes de ameaças e ataques cibernéticos.

Ademais, há grandes transformações tecnológicas ocorrendo no âmbito da Administração Pública federal, a exemplo do citado processo de TD, das terceirizações de serviços de tecnologia da informação (TI), da previsão de privatização de empresas públicas prestadoras de serviços de TI e de projetos de introdução de novas tecnologias (computação em nuvem, *big data*, internet das coisas, *blockchain*, inteligência artificial etc.). Todas essas transformações trazem consigo riscos relativos às questões de SegInfo e segurança cibernética (SegCiber) das organizações públicas.

Diante disso, a Secretaria de Fiscalização de Tecnologia da Informação (Sefti) realizou levantamento com vistas a entender a macroestrutura de governança e gestão de SegInfo e SegCiber da Administração Pública federal, incluindo legislação, políticas, normativos, atores, papéis e responsabilidades, levantar as principais ações em andamento, consolidar as informações disponíveis nessas áreas e identificar os principais riscos e vulnerabilidades envolvidos. Como consequência, propôs estratégia para que o Tribunal de Contas da União (TCU), ao longo dos próximos anos, acompanhe e induza a boa gestão de SegInfo e SegCiber na Administração.

A referida estratégia, descrita no presente documento, prevê a realização de ações e iniciativas específicas para ajudar a melhorar o panorama da Administração Pública federal nessas áreas, incluindo a realização de acompanhamento ágil de controles críticos de SegCiber, para conscientizar os órgãos como um todo quanto à importância dessas questões. A partir da sua execução, pretende-se fomentar uma cultura de SegInfo nos órgãos e nas entidades da Administração Pública federal e contribuir para que mantenham processos bem definidos de governança e gestão de SegInfo e SegCiber, minimizando, assim, riscos e possíveis impactos de ataques cibernéticos e incidentes de SegInfo.

Por fim, registra-se que, embora abrangente, essa estratégia não é exaustiva, podendo ocorrer a reavaliação de algumas das ações aqui previstas devido a eventuais restrições da Sefti ou de outras secretarias de controle externo quanto à disponibilidade de recursos humanos, bem como ser incluídas novas ações no decorrer da sua condução, a depender do contexto do momento e das respectivas viabilidade e oportunidade.

VISÃO GERAL DA ESTRATÉGIA

Conforme ilustra a Figura 1, a estratégia está alinhada a situação-problema descrita na Lista de Alto Risco da Administração Pública (LAR) 2019-2020 e a três objetivos estratégicos do Plano Estratégico do TCU (PET) 2019-2025.

Ademais, sua estrutura é dividida em quatro eixos, com três objetivos primordiais: i) posicionar o Brasil no topo do ranking do *Global Cybersecurity Index* (GCI), entre os países da América Latina; ii) disseminar uma cultura de SegInfo no seio do Estado e da sociedade como um todo; iii) contribuir para a definição e implementação de processos de governança e gestão de SegInfo e SegCiber nos órgãos e nas entidades da Administração Pública federal.

Figura 1 – Fundamentos da Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023

Situação-problema (cenário anterior)
LAR 2019-2020: a baixa governança sobre as informações produzidas e custodiadas pelo Estado afeta seu compartilhamento, sua qualidade e sua segurança.

PET 2019-2025 (alinhamento)		
47. Induzir o aperfeiçoamento da gestão de riscos e controles internos na APF	48. Contribuir para a transformação digital do país	50. Induzir a disponibilidade e a confiabilidade de informações na Administração Pública

Estratégia de SegInfo / SegCiber do TCU (4 eixos / linhas de ação)			
1 - Mapear a situação: atores, estruturas, normas, riscos e ações	2 - Diagnosticar a situação	3 - Induzir a adoção de boas práticas e o cumprimento de normas	4 - Acompanhar as ações

Cenário desejado (ao final de 4 anos)		
Brasil: país da América Latina melhor posicionado no ranking do GCI	Cultura de SegInfo amplamente disseminada no Estado e na sociedade	Processos de governança egestão de SegInfo/SegCiber bem definidos e implementados nos órgãos da APF

Fonte: TC 001.873/2020-2, relatório, Figura 35.

No que se refere às quatro linhas de ação previstas, tem-se:

Mapear situação: fiscalizações, tipicamente do tipo levantamento, destinadas a identificar, entre outros, atores, estruturas organizacionais, normas, ações em andamento, riscos e vulnerabilidades;

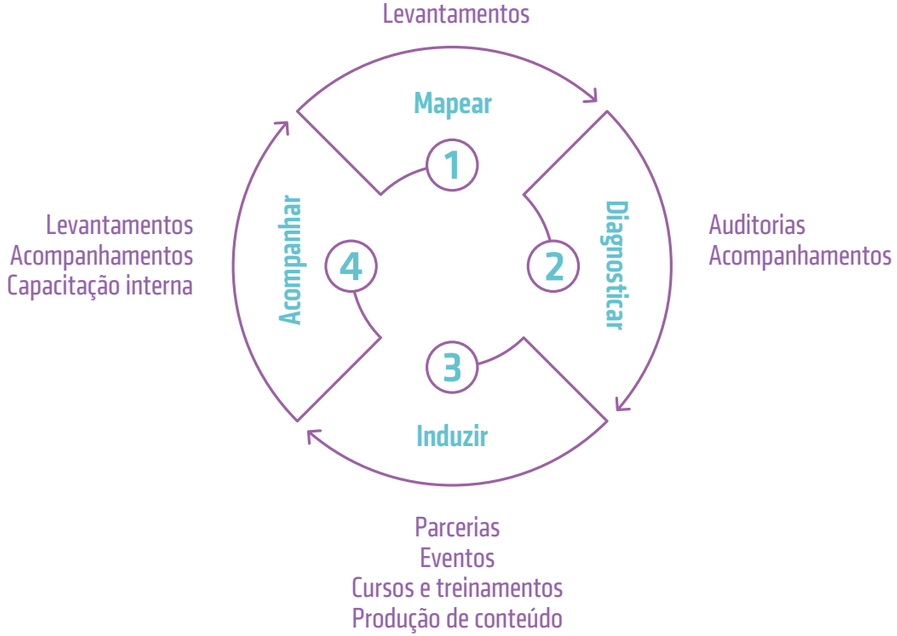
Diagnosticar situação: auditorias e acompanhamentos com escopo bem definido para diagnóstico e avaliação de temas e problemas específicos;

Induzir adoção de boas práticas e cumprimento de normas: formalização de parcerias com outros órgãos, organização de eventos, promoção de cursos e treinamentos, elaboração e publicação de conteúdos, enfim, atividades direcionadas à conscientização e educação dos gestores;

Acompanhar ações: atividades voltadas a assegurar a continuidade das iniciativas, envolvendo a capacitação contínua dos auditores da Sefti, a avaliação constante do cenário de ameaças e riscos e o acompanhamento da evolução da governança e gestão de SegInfo e SegCiber nos órgãos.

Ressalte-se que essas linhas de ação integram um processo cíclico e contínuo (Figura 2).

Figura 2 – Linhas de ação da Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023



Fonte: TC 001.873/2020-2, relatório, Figura 36.

A Figura 3, a título de sugestão, mostra uma linha do tempo com as ações previstas para serem executadas no primeiro ciclo da estratégia (2020-2023). Tais ações, no entanto, abordam temas distintos, sem relação de precedência, podendo ocorrer em outra ordem ou mesmo em paralelo.

Figura 3 – Linha do tempo da Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023

Fonte: TC 001.873/2020-2, relatório, Figura 37.

As seções a seguir, então, detalham cada uma dessas ações, divididas de acordo com as quatro linhas de atuação propostas, à exceção do TC 035.863/2019-6 (levantamento da governança e gestão de SegInfo e SegCiber na Administração Pública federal), de cujo relatório foi extraída esta estratégia.

EIXO I

MAPEAR SITUAÇÃO

I.1. Levantamento de riscos em sistemas informacionais da Administração Pública federal

Ação realizada pela Sefti (TC 031.436/2019-6), que identificou os sistemas críticos da Administração Pública federal e diagnosticou as capacidades de fiscalização de sistemas das unidades técnicas do TCU, tendo resultado no Acórdão 1.889/2020-TCU-Plenário (Rel. Min. Aroldo Cedraz).

I.2. Levantamento de infraestruturas críticas nacionais

Do mesmo modo que identificou os sistemas críticos da Administração Pública federal, o Tribunal também precisa mapear as infraestruturas críticas (ICs) nacionais (setores de telecomunicações, transportes, energia, água e financeiro), visto que tais instalações podem sofrer ataques cibernéticos, com potencial de causar danos graves, como acidentes e indisponibilidade de serviços essenciais.

Dentre os objetivos da Política Nacional de Segurança das Infraestruturas Críticas (PNSIC), destacam-se "a prevenção de eventual interrupção, total ou parcial, das atividades relacionados às [ICs] ou, no caso de sua ocorrência, a redução dos impactos dela resultantes" e "a integração de dados sobre ameaças, tecnologias de segurança e gestão de riscos" (Decreto 9.573/2018, Anexo, art. 3º, incs. I e III).

A seu turno, a Estratégia Nacional de Segurança Cibernética (E-Ciber) listou "Elevar o nível de proteção das ICs Nacionais" entre suas dez ações estratégicas, alertando que "os principais tipos de ameaças contra as [ICs] são ataques de *phishing*, negação de serviço em larga escala, vazamentos de informações privadas ou institucionais, espionagem cibernética e a interrupção de serviços" e que muitas estratégias nacionais de SegCiber mencionam os ataques às ICs "entre as maiores ameaças à segurança nacional" (Decreto 10.222/2020, Anexo, item 2.3.5, e Parte II, item 1.3).

Assim, este levantamento servirá para mapear as ICs nacionais, verificar a implementação da PNSIC e avaliar o quanto essas estruturas estão expostas e vulneráveis a ameaças cibernéticas. Em função da natureza do tema, a coordenação desta ação deverá ficar a cargo da Secretaria de Controle Externo da Defesa Nacional e da Segurança Pública (SecexDefesa), com participação da Sefti.

I.3. *Benchmarking* internacional

Esta ação consiste na realização de benchmarking para comparar as práticas nacionais de governança e gestão de SegInfo e SegCiber e, se possível, o orçamento nacional destinado a Defesa Cibernética (DefCiber) com as práticas e os valores adotados por nações tidas como referência nessas áreas, vizinhos da América Latina e outros países com nível de desenvolvimento similar ao do Brasil.

Após a elaboração dos instrumentos de coleta pela Sefti, a Secretaria de Relações Internacionais (Serint), com eventual apoio da Sefti ao longo da execução, se necessário, fará contatos com representações e entidades de outros países.

Além de identificar boas práticas, esta ação poderá incluir a realização de análise detalhada das avaliações individuais do Brasil em cada uma das cinco dimensões do GCI (aspectos legais, aspectos técnicos, aspectos organizacionais, construção de capacidade e cooperação), comparando-as às avaliações correspondentes de Paraguai, México e Uruguai, de modo a nortear o atingimento do objetivo de superação, pelo Brasil, desses países no referido ranking.

EIXO I I

DIAGNOSTICAR SITUAÇÃO

II.1. Auditoria sobre a LGPD

Auditoria com o objetivo de conscientizar os gestores e verificar o nível de preparo e conformidade das organizações públicas em relação às exigências da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), bem como avaliar a estruturação da Autoridade Nacional de Proteção de Dados (ANPD).

A abordagem utilizada será a autoavaliação de controles (*Control Self Assessment* – CSA), por meio da aplicação, aos gestores dos órgãos, de questionários abarcando os conceitos básicos (papéis e responsabilidades, princípios, direitos dos titulares dos dados e bases legais para o respectivo tratamento) e as etapas de implantação de um Sistema de Gestão de Proteção de Dados (SGPD). Os gestores, então, responderão os questionários, anexando documentos comprobatórios e justificativas para as deficiências, sendo todos esses materiais analisados e consolidados para confecção do relatório.

Além de avaliar o processo de implantação da LGPD na Administração Pública federal, essa auditoria servirá para despertar interesse quanto ao tema, produzir conhecimento especificamente voltado à sua implantação no setor público e nortear as atuações dos órgãos para o atingimento da conformidade com a lei.

Tendo em vista que a LGPD entrou em vigor em 18/9/2020, com a sanção da Lei 14.058/2020 (conversão da Medida Provisória 959/2020), a Sefti já iniciou os preparativos para realizar essa auditoria logo no início de 2021.

II.2. Auditoria em sistema crítico

Auditoria de sistema, avaliando, dentre outros aspectos, regras de negócio e SegInfo, em algum dos sistemas críticos identificados pela Sefti no âmbito do TC 031.436/2019-6 (item I.1) ou em sistema que suporte alguma das ICs a serem mapeadas em conjunto com a SecexDefesa (item I.2). Em qualquer dos casos, o sistema será selecionado com base em critérios de risco e oportunidade.

Idealmente, a Sefti poderá aproveitar a realização dessa auditoria para preparar um curso de capacitação básico em auditoria de sistemas, cobrindo os principais tópicos e pontos de atenção, a ser ministrado a auditores de outras unidades técnicas do Tribunal, com vistas a que essas unidades assumam, futuramente, a responsabilidade pela realização desse tipo de fiscalização sobre os sistemas dos órgãos que constituem suas clientelas.

II.3. Auditoria sobre *backup*

A fase de execução dessa auditoria (TC 036.620/2020-3 – Rel. Min. Vital do Rêgo) ocorreu entre os dias 15/10 e 13/11/2020, em parceria entre a Sefti e outras 12 unidades técnicas da Secretaria-Geral de Controle Externo (Segecex) do TCU, a saber: Secretaria de Controle Externo da Administração do Estado (SecexAdministração), Secretaria de Controle Externo da Agricultura e do Meio Ambiente (SecexAgroAmbiental), Secretaria de Controle Externo da Defesa Nacional e Segurança Pública (SecexDefesa), Secretaria de Controle Externo da Educação (SecexEducação), Secretaria de Controle Externo da Administração Indireta no Rio de Janeiro (SecexEstataisRJ), Secretaria de Controle Externo do Sistema Financeiro Nacional e dos Fundos de Pensão (SecexFinanças), Secretaria de Controle Externo da Saúde (SecexSaúde), Secretaria de Controle Externo do Trabalho e Entidades Paraestatais (SecexTrabalho), Secretaria de Fiscalização de Infraestrutura de Petróleo e Gás Natural (SeinfraPetróleo), Secretaria de Fiscalização de Infraestrutura Portuária e Ferroviária (SeinfraPortoFerrovia), Secretaria de Fiscalização de Infraestrutura Rodoviária e de Aviação Civil (SeinfraRodoviaAviação) e Secretaria de Fiscalização de Infraestrutura Urbana (SeinfraUrbana).

Em essência, foi utilizada a metodologia CSA, incluindo a solicitação de documentos comprobatórios (evidências), para avaliar se os procedimentos de *backup* e *restore* das organizações da Administração Pública federal, mais especificamente sobre suas principais bases de dados e sistemas críticos, são suficientes e adequados para garantir a continuidade dos serviços prestados. O respectivo relatório será finalizado em fevereiro de 2021.

Essa auditoria foi um "piloto" para o futuro acompanhamento de controles críticos de SegCiber, a ser realizado em parceria com a Secretaria de Infraestrutura de Tecnologia da Informação – Setic (item II.4 e Anexo I), tendo servido para validar a metodologia ágil de execução por meio da verificação de um controle específico, relativo aos processos de *backup* e *restore* dos órgãos da Administração Pública federal.

II.4. Acompanhamento de controles críticos de SegCiber

Fiscalização do tipo "acompanhamento", com vistas a obter dados e avaliar a adoção, pelos órgãos da Administração Pública federal, de controles considerados críticos para a gestão de SegCiber. Deverá ser utilizada metodologia ágil de gerenciamento de projetos, técnica que já vem sendo usada pela Sefti, com sucesso, em trabalhos de controle externo.

Em vista da tecnicidade do tema, essa ação, detalhada em seção específica adiante, deverá ser coordenada pela Sefti e contar com a participação da Setic, unidade do Tribunal especializada em TI e SegCiber.

II.5. Auditoria sobre identidade e assinatura digitais

Embora prevista no Brasil há anos, a identidade digital única dos cidadãos ainda não foi implantada, tanto por falta de entendimento político quanto pela enorme dificuldade de se sincronizar múltiplas bases governamentais, muitas das quais permeadas de inconsistências e incompletudes relativamente ao universo da população brasileira. Recentemente, inclusive, quando da necessidade de se implementar o pagamento do auxílio emergencial, devido à pandemia da covid-19, foi possível ter uma demonstração prática das consequências dessa deficiência sobre a gestão de políticas públicas.

A seu turno, a decisão pelo uso ou não de certificados digitais pode ser considerada um caso típico do dilema segurança *versus* facilidade de uso: por um lado, soluções mais seguras não são facilmente utilizáveis (*e.g.* assinaturas que utilizam certificados digitais da ICP-Brasil, cujo custo de emissão ainda é alto para a maioria da população e uso demanda certo conhecimento e aprendizado prévios); por outro, soluções com maior facilidade de uso podem ter sua validade jurídica questionada e/ou não fornecer o nível necessário de segurança (*e.g. login* e senha ou mesmo biometria).

Com isso, considerando-se o contexto de TD do Estado brasileiro e as necessidades de segurança e praticidade no que tange à implementação e gestão de políticas públicas, sugere-se a realização de auditoria com o fito de avaliar questões relativas à adoção de uma identidade civil única, digital e segura, bem como ao uso de assinaturas digitais da ICP-Brasil frente aos outros dois novos tipos de assinatura eletrônica, "simples" e "avançada", instituídos pela Medida Provisória (MPV) 983/2020.

Essa fiscalização deverá: i) considerar a necessidade de ampliação do acesso dos cidadãos brasileiros aos serviços digitais e o fato de que existem aplicações e serviços que não demandam, necessariamente, todos os requisitos de segurança impostos pela ICP-Brasil; ii) identificar e avaliar possíveis riscos de erros e fraudes decorrentes do uso das assinaturas eletrônicas "simples" e "avançada".

Considerando que o Tribunal já possui uma estratégia de atuação em TD (Acórdão 1.103/2019-TCU-Plenário – Rel. Min. Vital do Rêgo), a qual propôs fiscalização para acompanhamento das ações de suporte à desburocratização de serviços públicos por meio da TD, incluindo a implantação da Identidade Civil Nacional (ICN), sugere-se, como alternativa a ser avaliada pela Sefti, que as questões de SegInfo mencionadas sejam incluídas no contexto do referido acompanhamento.

II.6. Auditoria no processo de resposta a incidentes cibernéticos

Diante da situação detectada em pesquisa realizada com as Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIRs) sob coordenação do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), aquém da ideal, considera-se oportuna fiscalização para avaliar a capacidade de resposta a incidentes cibernéticos dos órgãos da Administração Pública federal.

Essa avaliação poderá ser feita por meio de auditoria específica sobre o assunto ou, alternativamente, incluída no escopo do citado acompanhamento de controles críticos de SegCiber, sendo que a primeira opção, certamente, permitirá abordar o problema com maior profundidade.

EIXO III

INDUZIR ADOÇÃO DE BOAS PRÁTICAS E CUMPRIMENTOS DE NORMAS

III.1. Parceria ENaDCiber

Formalizar acordo de cooperação técnica entre a Escola Nacional de Defesa Cibernética (ENaDCiber) e o Instituto Serzedello Corrêa (ISC) para organização e realização conjunta de eventos e oferecimento de cursos e treinamentos em SegInfo, SegCiber e DefCiber direcionados à comunidade do controle e aos demais gestores.

III.2. Evento para órgãos de controle e gestores

Organizar e conduzir diálogo público voltado aos órgãos de controle e gestores em geral com vistas a divulgar a visão do TCU, bem como os resultados das ações da Sefti no âmbito desta estratégia. Naturalmente, essa ação envolveria a participação tanto do ISC quanto da Assessoria de Relações Institucionais e Cerimonial (Aceri).

III.3. Capacitação de TCEs

Realizar evento de capacitação tendo como público-alvo auditores dos tribunais de contas estaduais (TCEs), de modo que os principais trabalhos possam ser replicados em âmbito estadual. Além de conceitos e conhecimentos teóricos sobre SegInfo e SegCiber, apresentar esta estratégia e os resultados obtidos pela Sefti até o momento, incluindo o compartilhamento de experiências, técnicas e ferramentas.

III.4. Elaboração e publicação de conteúdo de orientação aos gestores

Elaborar, com base nos trabalhos da Sefti, materiais de divulgação com o propósito de orientar os gestores públicos, a exemplo de artigos e nota técnica, além de revisar e atualizar a cartilha "Boas Práticas em Segurança da Informação", publicada pelo TCU em 2012. Naturalmente, a editoração, publicação e divulgação desses materiais ficariam a cargo da Secretaria de Comunicação (Secom).

EIXO IV

ACOMPANHAR AÇÕES

IV.1. Calcular iSegInfo derivado do iGG 2021

Em parceria com a SecexAdministração, revisar a forma de cálculo do Índice de Capacidade em Gestão de Segurança da Informação (iSegInfo), indicador derivado do Índice Integrado de Governança e Gestão (iGG), considerando a reformulação das perguntas do levantamento integrado de governança do TCU relacionadas a SegInfo e SegCiber resultante do TC 001.873/2020-2.

Esta ação será importante para instituir, a partir de 2021, forma padronizada (iSegInfo) para acompanhamento da evolução das práticas de gestão de SegInfo e SegCiber no âmbito da Administração Pública federal.

IV.2. Elaborar matriz de risco de SegInfo e SegCiber

Correlacionar informações de fontes variadas (*e.g.* iSegInfo, sistemas críticos da Administração Pública federal, levantamento de ICs nacionais, base de dados de incidentes do CTIR Gov) para elaborar matriz de risco de SegInfo e SegCiber e painel que servirão de subsídio à priorização de objetos de controle pela Sefti.

IV.3. Acompanhar evolução do iSegInfo

Compatibilizar os dados do ciclo 2018 do levantamento integrado de governança com a metodologia desenvolvida em parceria com a SecexAdministração para cálculo do iSegInfo (item IV.1), permitindo, assim, avaliar a evolução desse indicador de 2018 para 2021.

No âmbito do TC 001.873/2020-2, já foi desenvolvido painel que permite visualizar graficamente as informações do levantamento integrado de governança realizado pelo TCU. Com isso, a cada novo ciclo de aplicação do questionário, as novas informações recebidas serão incorporadas nesse painel, o que permitirá que a Sefti acompanhe a evolução do iSegInfo ao longo dos próximos anos.

IV.4. Acompanhar evolução do cenário de SegInfo e SegCiber

Sugere-se a construção de um painel que permita acompanhar a evolução dos eventos de SegInfo e da atividade cibernética maliciosa em andamento no país, o que seria viabilizado a partir da celebração de acordos de cooperação técnica com o CTIR Gov e, possivelmente, com o CERT.br, para obtenção, de forma contínua e periódica, de dados detalhados relativos às notificações de incidentes cibernéticos dos entes sob suas coordenações. Esses dados, então, poderão ser agregados a notícias e alertas de ameaças emitidos por essas e outras entidades, inclusive internacionais, possibilitando que a Sefti e o TCU atuem de modo proativo e tempestivo, em especial nas questões relacionadas a SegCiber.

Outra ação possível seria um acompanhamento mais aprofundado das questões de SegInfo e SegCiber no âmbito das grandes transformações em curso na Administração Pública federal, a exemplo do processo de TD e da introdução de novas tecnologias. Especificamente, essa fiscalização poderia avaliar o cumprimento da EGD 2020-2022 (Decreto 10.332/2020), em especial dos seus objetivos 10 (LGPD), 11 (segurança das plataformas de governo digital e de missão crítica) e 12 (identidade digital).

IV.5. Capacitar auditores do TCU em SegInfo e SegCiber

Esta ação visa a estimular a capacitação contínua dos auditores do TCU em SegInfo e SegCiber, por meio da obtenção de certificações profissionais e participação em cursos e eventos educacionais. A ideia é mapear, continuamente, esses cursos, esses eventos e essas certificações e elaborar, em parceria com o ISC, trilha de formação em auditoria de SegInfo e SegCiber, facilitando, por exemplo, o direcionamento de licenças-capacitação para essas atividades.

Anexo I

Acompanhamento ágil de controles críticos de SegCiber

Nesta seção, detalha-se a proposta de realização do acompanhamento ágil de controles críticos de SegCiber (item II.4), considerado essencial para conscientizar os órgãos da Administração Pública federal como um todo quanto à importância das questões de SegInfo e SegCiber.

Esta auditoria deverá ser realizada na forma de CSA, ferramenta já utilizada pelo TCU, com sucesso, nos levantamentos de governança e na "Auditoria sobre *backup*" (item II.3), aliada à metodologia ágil de gerenciamento de projetos. A realização do primeiro ciclo será, naturalmente, mais trabalhosa, devido à elaboração inicial dos instrumentos de coleta das informações, dos *templates* de e-mails e de outros documentos necessários. Contudo, a aplicação dos ciclos de avaliação seguintes será facilitada, podendo essa fiscalização ser repetida periodicamente, de modo a permitir o acompanhamento contínuo da evolução do cenário de SegCiber dos órgãos da Administração Pública federal.

Como já é de conhecimento do Tribunal, o uso de questionários *on-line* a ser preenchidos pelos gestores, além de prover ganho de escala na coleta de dados para o controle externo, pode ser, posteriormente, adaptado para disponibilização de serviço/ferramenta de autoavaliação contínua pelas próprias organizações públicas. Assim, esta auditoria envolve a elaboração de 20 questionários, baseados nos 20 controles críticos de SegCiber preconizados pelo *Center for Internet Security* (CIS), mostrados no Quadro 1.

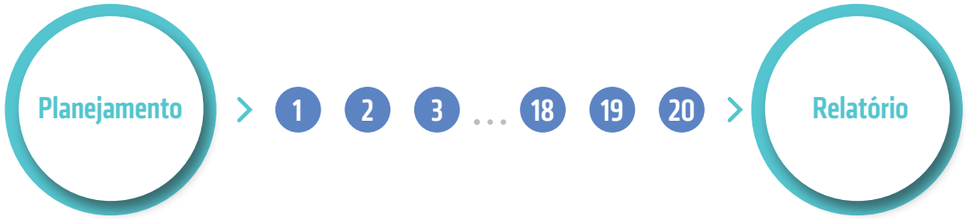
Quadro 1 – Controles críticos de SegCiber do *Center for Internet Security* (CIS)

Básicos	1	Inventário e controle de ativos de *hardware*
	2	Inventário e controle de ativos de *software*
	3	Gerenciamento contínuo de vulnerabilidades
	4	Uso controlado de privilégios administrativos
	5	Configuração segura de *hardware* e *software* em dispositivos móveis, *laptops*, estações de trabalho e servidores
	6	Manutenção, monitoramento e análise de *logs* de auditoria
	7	Proteção de *e-mail* e navegador da *web*
Fundamentais	8	Defesa contra *malware*
	9	Limitação e controle de portas, protocolos e serviços de rede
	10	Capacidade de recuperação de dados
	11	Configuração segura de dispositivos de rede (*firewalls*, roteadores, *switches* etc.)
	12	Defesa de perímetro
	13	Proteção de dados
	14	Controle de acesso com base na necessidade de saber (*need to know*)
	15	Controle de acesso sem fio (*wireless*)
	16	Monitoramento e controle de contas de usuário
Organizacionais	17	Programa de conscientização e treinamento em segurança
	18	Segurança de aplicações de *software*
	19	Resposta e gerenciamento de incidentes
	20	Teste de penetração e exercício de ataque (*red team exercises*)

Fonte: Disponível em: <https://www.cisecurity.org/controls/cis-controls-list>.

A fase de planejamento envolverá a elaboração dos 20 questionários, validação interna (Sefti e Setic) dos enunciados das perguntas e realização de teste dos procedimentos de coleta de dados. Durante a execução, os gestores responderão, a cada duas semanas, o questionário específico de autoavaliação do seu órgão a respeito de 1 (ou mais, caso seja oportuno aglutinar) dos 20 controles do CIS. Ao final, será elaborado o relatório consolidador, contendo panorama geral dos resultados obtidos, além de relatórios individuais de *feedback* a cada organização. A Figura 4 ilustra esse processo.

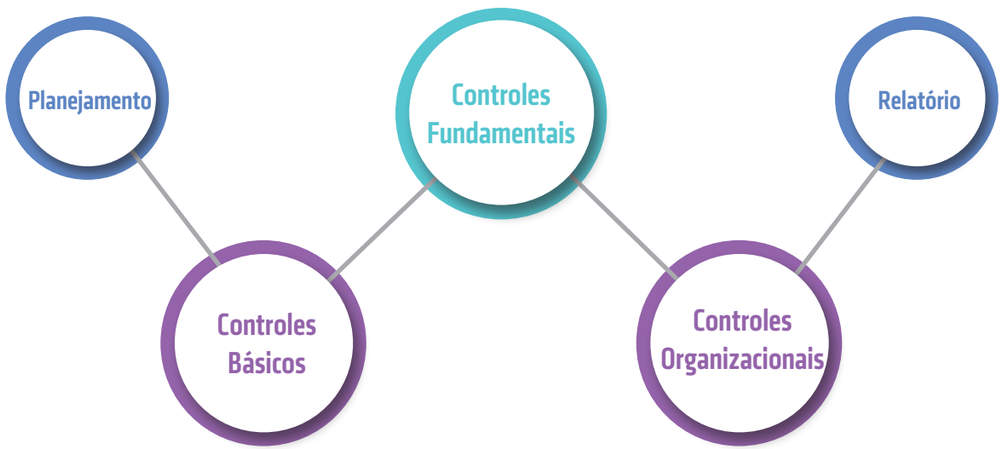
Figura 4 – Fases do "Acompanhamento de controles críticos de SegCiber"



Fonte: TC 001.873/2020-2, relatório, Figura 38.

A condução do trabalho será dividida em três grandes etapas, de acordo com as três categorias de controles do CIS: básicos, fundamentais e organizacionais (Figura 5).

Figura 5 – Três grandes etapas do "Acompanhamento de controles críticos de SegCiber"

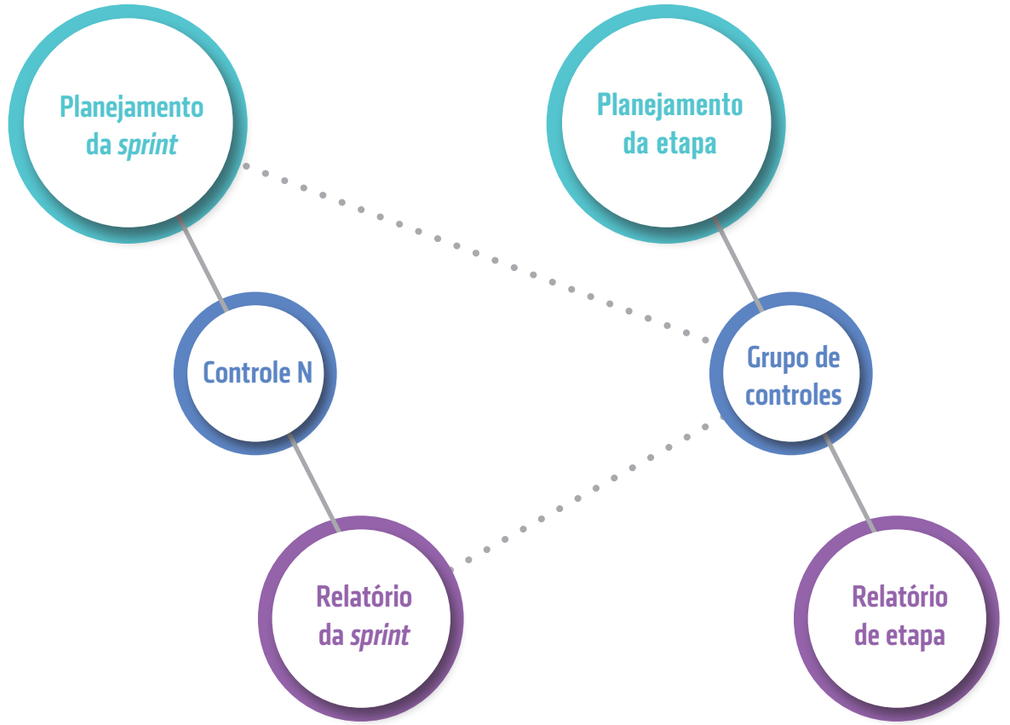


Fonte: TC 001.873/2020-2, relatório, Figura 39.

As autoavaliações serão executadas dentro de uma metodologia ágil, considerando que, em cada *sprint*, cuja duração será de duas semanas, os gestores responderão o questionário específico a respeito de 1 (eventualmente, mais de um, se houver aglutinação) dos 20 controles críticos do CIS.

Cada uma das *sprints* e etapas citadas será precedida de rápido planejamento individual, com revisão dos respectivos instrumentos de coleta e das mensagens antes do seu disparo, prevendo-se, ainda, a elaboração e o envio aos gestores de relatório parcial contendo o resultado da avaliação do(s) questionário(s) relativo(s) àquela *sprint*/etapa específica (Figura 6). Ou seja, além do relatório final, ao longo da execução serão gerados 20 (ou menos, se houver aglutinação) relatórios para as *sprints* e 3 relatórios parciais para os conjuntos de controles (básicos, fundamentais e organizacionais).

Figura 6 – Metodologia ágil na execução do "Acompanhamento de controles críticos de SegCiber"



Fonte: TC 001.873/2020-2, relatório, Figura 40.

Responsabilidade pelo conteúdo
Secretaria-Geral de Controle Externo
Secretaria de Fiscalização de Tecnologia da Informação

Projeto gráfico, diagramação e capa
Secretaria de Comunicação (Secom)
Núcleo de Criação e Editoração (NCE)

Tribunal de Contas da União
Secretaria-Geral da Presidência (Segepres)
SAFS Quadra 4 Lote 1
Edifício Sede Sala 146
70.042-900, Brasília – DF
(61) 3316-5338
segepres@tcu.gov.br

Ouvidoria do TCU
0800 644 1500
ouvidoria@tcu.gov.br

Impresso pela Senge/Segedam

Missão
Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo.

Visão
Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável.

TRIBUNAL DE CONTAS DA UNIÃO

TCU.GOV.BR