MINISTÉRIO DA ECONOMIA
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Governo Digital
Departamento de Governança de Dados e Informações
Coordenação-Geral de Segurança da Informação

Nota Técnica SEI nº 10726/2021/ME

Assunto: **Programa de Privacidade e Segurança da Informação para os Sistemas Informacionais Críticos da Administração Pública Federal Direta, Autárquica e Fundacional.**

Processo SEI/ME nº 19974.100460/2021-91

INTRODUÇÃO

1. O Decreto nº 10.332, de 28 de abril de 2020, instituiu a **Estratégia de Governo Digital (EGD)** para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Neste contexto, cabe à Secretaria de Governo Digital (SGD) da Secretaria Especial de Desburocratização, Gestão e Governo Digital (SEDGG), do Ministério da Economia, coordenar as ações para alcance dos objetivos de **implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do governo federal** e **de garantia da segurança das plataformas de governo digital e de sistemas de missão crítica**.

2. Em adição, a **Estratégia de Fiscalização do Tribunal de Contas da União (TCU) em Segurança da Informação e Segurança Cibernética** para o período de 2020-2023, apresentou 4 linhas de ações: a) mapear a situação (atores, estruturas, normas, riscos e ações); b) diagnosticar a situação (realização de auditorias); c) induzir (adoção de boas práticas e o cumprimento de normas); e d) acompanhar (acompanhamento das ações). Corroborando com a citada estratégia, um conjunto de acórdãos são considerados basilares: **Acórdão 1.889/2020-TCU-Plenário** (Auditoria sobre Sistemas Informacionais Críticos), **Acórdão 1.109/2021-Plenário** (Auditoria sobre Backups) e **Acórdão 1.784/2021-Plenário** (Auditoria sobre Estratégias de Transformação Digital da Administração Pública).

3. Nesse contexto, o **Acórdão 1.889/2020-TCU-Plenário,** resultado do processo de auditoria conduzida pelo TCU teve como objetivos **identificar os sistemas informacionais críticos da Administração Pública Federal** e **elaborar diagnóstico da capacidade de fiscalização de suas unidades técnicas com foco em sistemas**, o que resultou em orientações para corpo técnico do TCU, SGD/ME e para **58 órgãos integrantes do SISP.**

4. Dessa forma, a presente nota técnica objetiva fornecer subsídios às autoridades e gestores da administração pública federal direta, autárquica e fundacional, quanto ao processo de identificação, estabelecimento e gerenciamento dos controles internos de privacidade e segurança da informação, no que concerne aos sistemas informacionais computadorizados críticos, apontados no âmbito do **Acórdão: 1.889/2020-TCU-Plenário.**

5. O presente trabalho reveste-se de caráter contributivo para as autoridades, gestores, e em última instância, para os cidadãos, considerando-se a criticidade que os referidos sistemas informacionais desempenham no alcance dos objetivos institucionais dos órgãos integrantes do Sistema de Administração de

Recursos de Tecnologia da Informação (SISP), bem como no provimento de serviços públicos de qualidade para os cidadãos, no contexto da transformação digital do Estado brasileiro.

6. O presente documento busca contextualizar os gestores no que diz respeito aos desafios de adequação dos sistemas informacionais críticos quanto aos aspectos da privacidade e segurança da informação. Destaca-se que especial atenção deve ser dispensada à proteção de dados pessoais e sensíveis dos cidadãos, além dos aspectos relativos à segurança da informação. Ainda no documento, fornecem-se as diretrizes federais quanto à temática da governança e gestão de riscos, apresenta-se um breve resumo da legislação aplicada às temáticas da privacidade e segurança da informação, e ressalta-se o papel de órgãos federais de controle e de fiscalização na temática debatida. Também são apresentados, frente aos desafios indicados na EGD, soluções concretas e benefícios esperados para os órgãos integrantes do SISP, por meio do engajamento ao **Programa de Privacidade e Segurança da Informação,** liderado pela Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

ANÁLISE

I. DA CONTEXTUALIZAÇÃO

7. Um governo centrado nos cidadãos, que busca oferecer uma jornada mais agradável no acesso aos serviços digitais e responde às suas expectativas por meio da prestação de serviços de alta qualidade, deverá assegurar que os aspectos ligados à privacidade, com especial atenção à proteção de dados pessoais e sensíveis dos cidadãos, e os relacionados à segurança da informação, tornem-se centrais na Estratégia de Governo Digital (EGD).

8. Assim, a EGD apresenta, dentre seus objetivos, os importantes marcos de implementar a Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Governo federal e de garantir a segurança das plataformas de governo digital. Tais objetivos devem ser perseguidos por todos os gestores integrantes do Sistema de Administração de Recursos de Tecnologia da Informação (SISP). Materializando-se como tarefas bastantes desafiadoras frente ao ineditismo do tema da proteção de dados pessoais e sensíveis, trazidos pela LGPD, além do preocupante cenário, no qual órgãos públicos convivem diuturnamente com ameaças cibernéticas com potencial de afetar suas operações de forma parcial, ou até mesmo interromper completamente a prestação dos serviços públicos aos cidadãos.

9. Logo, é crucial planejar, organizar, liderar e monitorar as estratégias de adequação dos sistemas informacionais governamentais, quanto aos aspectos da privacidade e segurança da informação, com enfoque em um processo contínuo, incremental e colaborativo de amadurecimento da gestão de dados no âmbito da Administração Pública Federal. Os cidadãos, como controladores de seus dados, precisam estar seguros que suas informações disponíveis nas bases de dados governamentais serão confiáveis, íntegras, disponíveis e autênticas, reforçando as relações de transparência e confiança entre o governo e os cidadãos destinatários das políticas públicas.

10. Tal cenário poderá ser alcançado por meio da implementação de um conjunto de ações estruturadas em um Programa de Privacidade e Segurança da Informação, fortemente alicerçada por uma estratégia que trate das medidas de adequação em termos de privacidade e segurança da informação, de um modo transversal, concomitante, multidisciplinar e orientado para resultados. Assim, é proposto um modelo baseado em 5 (cinco) torres, que tem como enfoque a articulação simultânea das temáticas de Governança, Pessoas, Metodologia, Tecnologia e Gestão de Maturidade, nos sistemas informacionais críticos dos órgãos integrantes do SISP.

II. DA GOVERNANÇA E DA GESTÃO DE RISCOS

11. O **Decreto nº 9.203, de 22 de novembro de 2017**, dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. O referido Decreto define governança pública

como o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade, bem como apresenta o conceito de gestão de riscos como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

12. O Decreto em questão destaca como **diretrizes da governança pública** dois comandos relacionados ao contexto do presente documento: *"direcionar ações para a busca de resultados para a sociedade, encontrando soluções tempestivas e inovadoras para lidar com a limitação de recursos e com as mudanças de prioridades, bem como implementar controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores".*

13. Tal norma fornece direcionadores para a alta administração das organizações da administração pública federal direta, autárquica e fundacional, que deverão estabelecer, manter, monitorar e aprimorar sistemas de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os princípios indicados no decreto.

14. Logo, fica clara a importância da discussão, da implementação e do monitoramento dos comandos previstos no Decreto nº 9.203, de 22 de novembro de 2017, no que tange às boas práticas de governança pública e gestão de riscos, no âmbito dos órgãos integrantes do SISP. Mais uma vez, isso envolve especial atenção ao processo de identificação, estabelecimento e gerenciamento dos controles internos de privacidade e segurança da informação dos sistemas informacionais computadorizados críticos apontados no âmbito do **Acórdão: 1.889/2020-TCU-Plenário**.

III. DA LEGISLAÇÃO APLICADA

15. Considerando a lógica contributiva do presente documento, passam a ser destacadas algumas referências normativas que deverão fazer parte das discussões, das reflexões e do planejamento do Programa de Privacidade e Segurança da Informação a ser implementada pelos órgãos integrantes do SISP. Tais orientações não buscam esgotar a totalidade de normativos relativos à privacidade e à segurança da informação, constituindo apenas um facilitador para os gestores na construção, na implementação e no monitoramento do conjunto de ações que integrarão o Programa de Privacidade e de Segurança da Informação no âmbito dos órgãos.

16. Na frente de **Privacidade**, com especial atenção à **proteção de dados pessoais e sensíveis dos cidadãos**, passamos a destacar as seguintes normas federais:

1. **Lei Nº 12.527, de 18 de novembro de 2011**, Lei de Acesso à Informação (LAI), que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
2. **Lei Nº 12.965, de 23 de abril de 2014**, Marco Civil da Internet (MCI), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.
3. **Lei Nº 13.709, de 14 de agosto de 2018**, Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
4. **Decreto Nº 10.046, de 09 de outubro de 2019,** Governança no Compartilhamento de Dados (GCD), que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

5. **Decreto Nº 10.474, de 22 de agosto de 2020,** Estrutura Regimental da Autoridade Nacional de Proteção de Dados, que dispõe que a Autoridade Nacional de Proteção de Dados - ANPD, órgão integrante da Presidência da República, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pelo disposto na Lei nº 13.709, de 14 de agosto de 2018.
6. **Instrução Normativa SGD/ME Nº 117, de 19 de novembro de 2020**, que dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.
7. **Portaria ANPD Nº 11, de 27 de janeiro de 2021,** Agenda Regulatória para o biênio 2021-2022, que torna pública a Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD) para o biênio 2021-2022, na forma do Anexo a esta Portaria, aprovada pelo Conselho-Diretor na Reunião Deliberativa nº 1.
8. **Instrução Normativa SGD/ME Nº 31, de 23 de março de 2021,** Requisitos e Obrigações quanto à Segurança e Privacidade, que altera a Instrução Normativa nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
9. **Resolução CD/ANPD Nº 1, de 28 de outubro de 2021,** que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados - ANPD.
10. **Documentos e Publicações da Autoridade Nacional de Proteção de Dados (ANPD)** disponíveis em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes .
11. **Documentos e Publicações da Secretaria de Governo Digital (SGD) do Ministério da Economia** disponíveis em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd .

17. Na frente de **Segurança da Informação**, com especial atenção quanto à **segurança cibernética**, passa-se a destacar as seguintes normas:

1. **Lei Nº 12.737, de 30 de novembro de 2012**, que dispõe sobre a tipificação criminal de delitos informáticos (Crime de Invasão de Dispositivo Informático), altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
2. **Lei Nº 13.709, de 14 de agosto de 2018**, Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
3. **Decreto Nº 9.573, de 22 de novembro de 2018,** Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), que tem por finalidade garantir a segurança e a resiliência das infraestruturas críticas do País e a continuidade da prestação de seus serviços.
4. **Decreto Nº 9.637, de 26 de dezembro de 2018,** Política Nacional de Segurança da Informação (PNSI), que dispõe sobre a governança da segurança da informação.
5. **Decreto Nº 10.222, de 05 de fevereiro de 2020,** Estratégia Nacional de Segurança Cibernética (E-CIBER), que dispõe sobre orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.
6. **Instrução Normativa GSI Nº 4, de 26 de março de 2020,** que dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.
7. **Instrução Normativa GSI Nº 1, de 27 de maio de 2020,** que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
8. **Instrução Normativa GSI Nº 2, de 24 de julho de 2020,** que altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
9. **Instrução Normativa SGD/ME Nº 31, de 23 de março de 2021,** Requisitos e Obrigações quanto à Segurança e Privacidade) , que altera a Instrução Normativa nº 1, de 4 de abril de 2019, que dispõe sobre o processo de

contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

10. **Instrução Normativa GSI Nº 3, de 28 de maio de 2021,** que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
11. **Decreto Nº 10.748, de 16 de julho de 2021,** Rede Federal de Gestão de Incidentes Cibernéticos, que dispõe sobre a instituição da Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do disposto no inciso VII do **caput** do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018.
12. **Instrução Normativa GSI Nº 5, de 31 de agosto de 2021,** que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
13. **Portaria GSI/PR Nº 93, de 18 de outubro de 2021,** Glossário de Segurança da Informação, que dispõe sobre a aprovação do Glossário de Segurança da Informação, na forma do Anexo a esta Portaria.

14. **Documentos e Publicações da Autoridade Nacional de Proteção de Dados (ANPD)** disponíveis em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes .
15. **Documentos e Publicações da Secretaria de Governo Digital (SGD) do Ministério da Economia** disponíveis em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd .

IV. DOS ÓRGÃOS DE CONTROLE E FISCALIZAÇÃO

18. Ademais, devem ser recordados os papéis institucionais da Autoridade Nacional de Proteção de Dados (ANPD), Ministério Público Federal (MPF), Tribunal de Contas da União (TCU) e Controladoria-Geral da União (CGU) no desempenho de suas funções de controle externo e controle interno, considerando as respectivas normas exaradas pelos órgãos de fiscalização, relativas à temática da privacidade e segurança da informação, no cumprimento de suas missões institucionais. São destacados alguns normativos e deliberações, de observância obrigatória pelos órgãos da Administração Pública Federal, conectados com o escopo da presente nota técnica.

19. Dessa forma, passa-se à análise das orientações exaradas pelo Tribunal de Contas da União (TCU) referentes às questões de privacidade e segurança da informação, em especial, a **Estratégia de Fiscalização do TCU em Segurança da Informação e Segurança Cibernética para o período de 2020-2023**. De tal documento, foram extraídos relevantes trechos para reflexão dos gestores integrantes do SISP, compartilhados a seguir:

> *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.*

20. A Estratégia de Fiscalização do TCU em Segurança da Informação e Segurança Cibernética para o período de 2020-2023 apresenta 4 linhas de ações: a) mapear a situação: atores, estruturas, normas, riscos e ações; b) diagnosticar a situação: realização de auditorias; c) induzir: adoção de boas práticas e o cumprimento de normas; e d) acompanhar: acompanhamento das ações. Tal estratégia sinaliza para os órgãos integrantes do SISP quais as ações relacionadas à Privacidade e Segurança da Informação já foram realizadas (auditoria em sistemas críticos, auditoria sobre backup, etc), quais estão em curso (auditoria sobre LGPD) e aquelas planejadas para o futuro (auditoria no processo de resposta a incidentes cibernéticos).

21. Por tal razão, recomenda-se aos órgãos integrantes do SISP o estudo detido sobre a Estratégia de Fiscalização do TCU em Segurança da Informação e Segurança Cibernética, considerando as recomendações e determinações já exaradas no âmbito das auditorias já concluídas pela egrégia corte, destacando-se como exemplos as seguintes deliberações do Tribunal: Acórdão 1.889/2020-TCU-Plenário (Auditoria sobre Sistemas Informacionais Críticos), Acórdão 1.109/2021-Plenário (Auditoria sobre Backups) e Acórdão 1.784/2021- Plenário (Auditoria sobre Estratégias de Transformação Digital da Administração Pública).

22. Nesse contexto, no período de **outubro/2019 a fevereiro/2020**, o Tribunal de Contas da União (TCU) realizou auditoria para identificar os sistemas informacionais críticos da Administração Pública Federal e elaborar diagnóstico da capacidade de fiscalização de suas unidades técnicas com foco em sistemas. O referido trabalho resultou na publicação do **Acórdão 1.889/2020-TCU-Plenário** com orientações aos **58 órgãos integrantes do SISP** que participaram da referida auditoria conduzida pelo TCU.

23. Assim, apresentam-se abaixo as principais conclusões e informações adicionais do **Relatório de Levantamento de Auditoria** da **equipe técnica do TCU (Páginas 30-32)**:

> *A presente fiscalização buscou identificar **os sistemas informacionais críticos da Administração Pública Federal** e elaborar diagnóstico da capacidade de fiscalização das unidades técnicas com foco em sistemas, de modo a subsidiar o desenvolvimento de estratégia para fiscalizar sistemas que considere a capacidade e responsabilidade de cada uma das unidades.*
>
> *Acerca da identificação dos sistemas críticos, foi **construída metodologia para determinação do nível de criticidade dos sistemas** com base em conjunto de parâmetros agrupados em duas dimensões: **Impacto** (decorrente de incidente de segurança da informação ou falha do sistema) e **Vulnerabilidade** (suscetibilidade do sistema ou do ambiente em que ele opera de ter sua disponibilidade, integridade ou confidencialidade comprometida).*
>
> *O levantamento de informações acerca dos parâmetros foi realizado por meio de questionário autoavaliativo aplicado junto aos **58 órgãos/entidades participantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp)** selecionados para escopo da fiscalização.*
>
> *O trabalho reuniu **279 sistemas relevantes**, conforme seleção realizada pelas próprias unidades jurisdicionadas pesquisadas seguindo orientação da equipe de fiscalização, que, após a aplicação do modelo de avaliação de criticidade, foram classificados desta forma: a) **45** sistemas críticos, assim considerados aqueles de **alta criticidade (16%)**; b)* **93** sistemas classificados como no nível de **criticidade média (33%)**; e c) **141** sistemas classificados como de **criticidade baixa (51%).**
>
> *A Sefti, de posse das informações desse levantamento, **elaborará estratégia de auditoria de sistemas críticos em conjunto com as unidades técnicas, com previsão de incluir nesse plano operacional a primeira auditoria de sistema decorrente das informações do trabalho**.*
>
> *No decorrer da fiscalização, a equipe de fiscalização recebeu solicitação da Coordenação-Geral de Arquitetura de Dados e Informações, vinculada à **Secretária de Governo Digital do***

***Ministério da Economia (SGD/ME)**, para fornecimento de dados brutos obtidos na pesquisa de sistemas críticos.*

***Tendo em vista as atribuições e responsabilidades da SGD** destacadas anteriormente, bem como o fato de a solicitação tratar de dados brutos recebidos dos órgãos/entidades participantes do Levantamento ora tratados como públicos, **propõe-se o encaminhamento de planilha consolidada com o conjunto de informações obtido das organizações à Coordenação-Geral de Arquitetura de Dados e Informações da SGD/ME**.*

24. Adicionalmente, destacam-se as recomendações do **Acórdão 1.889/2020-TCU-Plenário:**

*VISTOS, relatados e discutidos estes autos de Levantamento de Auditoria com o objetivo de **identificar os sistemas informacionais críticos da Administração Pública Federal** e **elaborar diagnóstico da capacidade de fiscalização das unidades técnicas com foco nos sistemas críticos**;*

ACORDAM os ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, ante as razões expostas pelo relator, em:

9.1. recomendar ao Tribunal de Contas da União que elabore, em até 120 (cento e vinte dias), estratégia de fiscalização de sistemas críticos, a qual preveja, entre outros assuntos relevantes:

9.1.1. os riscos incorporados pelas transformações tecnológicas em andamento;

9.1.2. a mitigação dos riscos oriundos das lacunas apontadas no presente Relatório de Levantamento em sua capacidade de fiscalização;

***9.1.3. a priorização de ações de controle dos sistemas identificados, conforme critérios de avaliação de risco**;*

***9.1.4. a possibilidade de ser recomendado aos órgãos e entidades responsáveis por sistemas críticos que realizem auditorias nos referidos sistemas, sem prejuízo de acompanhamento por parte deste Tribunal**;*

9.2. autorizar a Secretaria de Fiscalização de Tecnologia da Informação (Sefti) a:

a: 9.2.1. disponibilizar painel de informações acessível às Secretarias de Controle Externo que permita consultar e cruzar dados produzidos neste levantamento com vistas a subsidiar decisões acerca da estratégia de análise e tratamento de dados dessas unidades e o planejamento de fiscalizações envolvendo Sistemas de Informação;

9.2.2. compartilhar a metodologia desenvolvida no presente levantamento;

9.2.3. compartilhar as informações referentes à classificação dos sistemas por criticidade na forma de relatórios gerenciais, sem a identificação de sistemas específicos;

9.3. encaminhar à Coordenação-Geral de Arquitetura de Dados e Informações, da Secretaria de Governo Digital do Ministério da Economia (SGD/ME), cópia de planilha com os dados brutos recebidos dos órgãos/entidades fiscalizados;

9.4. encaminhar a metodologia de avaliação de criticidade dos sistemas e a classificação dos sistemas considerados críticos ou relevantes às respectivas organizações responsáveis, de forma que cada organização tenha conhecimento da classificação de criticidade dos sistemas sob sua responsabilidade;

9.5. manter o sigilo sobre o presente processo, conforme previsto no art. 9º, inciso VIII, da Resolução-TCU 294/2018, com exceção do presente Acórdão, do Voto e do Relatório que o fundamenta;

9.6. arquivar os presentes autos, nos termos do art. 169, inciso V, do Regimento Interno do TCU.

V. DA RECOMENDAÇÃO DA SECRETARIA DE GOVERNO DIGITAL DO MINISTÉRIO DA ECONOMIA

25. Diante de todas as informações acima elucidadas, e considerando que o **Art. 132 do Anexo I do Decreto nº 9.745, de 08 de abril de 2019**, no qual são descritas as competências da **Secretaria de Governo Digital**, destaca as seguintes atribuições: *I - atuar como órgão central do Sisp; IV - apoiar ações de fomento a segurança da informação e proteção a dados pessoais no âmbito da administração pública federal, em articulação com os órgãos responsáveis por essas políticas;*

26. Considerando os **objetivos 10 e 11**, do **Decreto nº 10.332, de 28 de abril de 2020,** que institui a **Estratégia de Governo Digital para o período de 2020 a 2022,** que destacamos: *Objetivo 10 - Implementação da Lei Geral de Proteção de Dados no âmbito do Governo federal e Objetivo 11: Garantia da segurança das plataformas de governo digital e de missão crítica;*

27. *Considerando as recomendações exaradas no âmbito do* **Acórdão 1.889/2020-TCU-Plenário,** em especial:

9.1. recomendar ao Tribunal de Contas da União que elabore, em até 120 (cento e vinte dias), estratégia de fiscalização de sistemas críticos, a qual preveja, entre outros assuntos relevantes:

9.1.3. a priorização de ações de controle dos sistemas identificados, conforme critérios de avaliação de risco;

9.1.4. a possibilidade de ser recomendado aos órgãos e entidades responsáveis por sistemas críticos que realizem auditorias nos referidos sistemas, sem prejuízo de acompanhamento por parte deste Tribunal;

9.3. encaminhar à Coordenação-Geral de Arquitetura de Dados e Informações, da Secretaria de Governo Digital do Ministério da Economia (SGD/ME), cópia de planilha com os dados brutos recebidos dos órgãos/entidades fiscalizados; e

9.4. encaminhar a metodologia de avaliação de criticidade dos sistemas e a classificação dos sistemas considerados críticos ou relevantes às respectivas organizações responsáveis, de forma que cada organização tenha conhecimento da classificação de criticidade dos sistemas sob sua responsabilidade.

28. A Secretaria de Governo Digital (SGD) recomenda aos órgãos integrantes do Sistema de Administração de Recursos de Tecnologia da Informação (SISP) as seguintes ações relacionadas ao Programa de Privacidade e Segurança da Informação:

1. Estudo, implementação e monitoramento das ***legislações relativas à Privacidade e Segurança da Informação destacadas nos itens 13 e 14 da presente nota técnica****, sem prejuízo da adoção das demais normas nacionais e internacionais, que direta ou indiretamente, contribuem para elevação do grau de maturidade da instituição em termos de Privacidade e Segurança da Informação.*

2. Estudo, implementação e monitoramento sobre a ***Resolução CD/ANPD Nº 1, de 28 de outubro de 2021,*** *que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.*

*3. Estudo, implementação e monitoramento sobre a **Estratégia de Fiscalização do TCU em Segurança da Informação e Segurança Cibernética para o período de 2020-2023**, com especial atenção quanto aos resultados das auditorias sobre Privacidade e Segurança da Informação já concluídas, em desenvolvimento e planejadas para 2022, no âmbito da referida estratégia.*

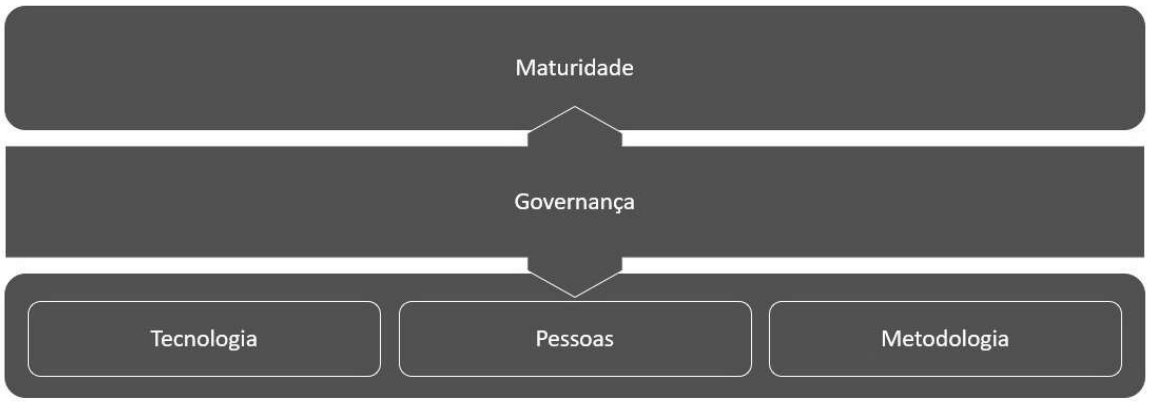
*4. Estudo, implementação e monitoramento do **Acórdão 1.889/2020-TCU-Plenário**, com especial atenção quanto aos sistemas informacionais críticos mapeados pelo TCU, no âmbito da organização, com possíveis detalhamentos das ações até o momento empreendidas, em desenvolvimento e planejadas quanto ao tema.*

5. *Engajamento dos órgãos do SISP no **Programa de Privacidade e Segurança da Informação.***

VI. DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

29. O **Programa de Privacidade e Segurança da Informação** objetiva elevar o grau de maturidade, em termos de proteção de dados pessoais e sensíveis e ações de segurança da informação, dos órgãos integrantes do SISP, aumentando a proteção dos sistemas críticos de governo no ambiente cibernético.

30. O referido programa é composto por um conjunto de ações articuladas nas torres de **Governança, Pessoas, Metodologia, Tecnologia e Gestão de Maturidade,** direcionadas para os sistemas informacionais críticos descritos no **Acórdão 1.889/2020-TCU-Plenário.** Assim, passa-se a descrição sumarizada dos elementos mínimos a serem exploradas nas cinco dimensões do Programa:



Modelo do Programa de Privacidade e Segurança da Informação

31. Na **torre de governança**, abordaremos questões ligadas à identificação, ao estabelecimento e ao envolvimento dos principais atores do processo de busca por conformidade em privacidade, com especial atenção à proteção de dados pessoais e sensíveis dos cidadãos, e segurança da informação, tais como o responsável pela unidade de TIC, encarregado pelo tratamento dos dados pessoais, gestor de segurança, assessor de controle interno e ou equivalentes, dentre outros. Para além disso, buscar-se-á a construção de estratégias para implementação e monitoramento do Programa de Privacidade e Segurança da Informação por meio envolvimento da alta administração, reuniões de mensais de monitoramento, além da formalização dos resultados por meio de estabelecimento de entregas claras, tangíveis e monitoráveis. A referida torre buscará manter em perspectiva, junto à alta administração dos órgãos integrantes do SISP, as importantes temáticas da privacidade e segurança da informação, considerando-se o caráter cogente dos normativos e ações de controle de órgãos como ANPD, MP, TCU, CGU, ME e GSI, dentre outros.

32. Na **torre de pessoas**, focaremos nas importantes temáticas da cultura organizacional, processos de liderança e motivação, além de capacitações ligadas às competências técnicas e àquelas ligadas

à conformidade em privacidade e segurança da informação. Entende-se ser central a disseminação da cultura de privacidade, com especial atenção à proteção de dados pessoais e sensíveis dos cidadãos, e segurança da informação dentro das organizações, passando pelas importantes etapas de sensibilização dos colaboradores, modificação de padrões vigentes e adoção de novos padrões. Tais processos devem ser liderados pelo responsável pela unidade de TIC, encarregado pelo tratamento dos dados pessoais, gestor de segurança, assessor de controle interno e ou equivalente, dentre outros, cada qual em sua esfera de atuação. Tais líderes precisarão motivar suas equipes e fomentar a capacitação dos servidores públicos dos órgãos, além da sensibilizar a alta administração quanto à importância da temática da privacidade e segurança da informação. São esperadas desses líderes e das equipes envolvidas características como conhecimentos técnicos, inteligência emocional, organização, entusiasmo, empenho e resiliência. Por fim, o alcance dos objetivos esperados na torre passará por ações de capacitações que serão estruturados em trilhas de conhecimentos em privacidade e segurança da informação. As referidas trilhas já contam com um conjunto de cursos, guias, oficinas e workshops desenvolvidos pela SGD/ME, que serão complementados com novos materiais ao longo do ano de 2022.

33. Na **torre de metodologia**, implementaremos as 6 (seis) etapas que compõem essa torre, a saber:

33.1. Programa de Governança em Privacidade, de que trata o Guia de Elaboração de Programa de Governança em Privacidade de 2020;

33.2. Diagnósticos em Privacidade e Segurança da Informação;

33.3. Inventário de Dados Pessoais;

33.4. Planos de Adequação à LGPD, conforme os 12 guias de boas práticas publicados pela SGD/ME;

33.5. Estratégias de Implementação; e

33.6. Monitoramento.

34. Na **torre de tecnologia**, focaremos nas seguintes frentes:

34.1. Soluções em segurança cibernética, contemplando avaliação e fomento da adoção de ferramentas de diagnósticos dos sistemas críticos que permitam a aplicação de testes como PENTEST, SAST, DAST, bem como prospecção conjunta com os órgãos do SISP de soluções SOC (*Security Operations Center*), SIEM (Security Information and Event Management) e NOC (*Network Operations Center*), dentre outras;

34.2. Atuação coordenada e sinérgica com os centros de segurança do SERPRO e DATAPREV para potencializar a adoção e ganho de escala das ferramentas de segurança cibernética, bem como para realização de diagnósticos e testes na identificação de vulnerabilidades nos sistemas de missão crítica;

34.3. Desenvolvimento de plataforma de consentimento do cidadão para atendimento a princípios preconizados na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), além de outras ferramentas.

35. Na **torre de gestão de maturidade**, serão aplicados mecanismos para avaliação e gestão do grau de proteção dos sistemas no ambiente cibernético. Tais mecanismos são constituídos pelos índices de maturidades em privacidade e segurança da informação, que subsidiarão o órgão na construção, na implementação e no monitoramento de seu Programa de Privacidade e Segurança da Informação. Destacando-se que a referida classificação objetiva exclusivamente balizar os trabalhos de planejamento, implementação e monitoramento, não configurando-se como uma certificação emitida pela Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital, do Ministério da Economia.

VII. DOS BENEFÍCIOS ESPERADOS E DOS FATORES CRÍTICOS DE SUCESSO

36. A implementação do Programa de Privacidade e Segurança da Informação trará uma série de benefícios, tais como:

a) Ampliação da confiabilidade e da proteção de sistemas informáticos contra incidentes de segurança;

b) Garantia da privacidade dos dados pessoais dos cidadãos inseridos nas bases de dados governamentais;

c) Aumento da confiança da população na prestação de serviços digitais por parte do governo federal;

d) Disseminação da cultura de proteção de dados e segurança da informação na organização;

e) Identificação, tratamento e controle dos riscos mais significativos em cada sistema informacional crítico do órgão;

f) E, por fim, avanço no processo de transformação digital dos serviços de governo, com possibilidade de melhoria na qualidade, redução de custos e de prazos, nos serviços públicos ofertados pelos órgãos integrantes do SISP.

37. Destacam-se como fatores críticos de sucesso para a implementação do Programa de Privacidade e Segurança da Informação:

a) O suporte da alta administração ao programa;

b) O engajamento dos atores chave, a saber: do responsável pela unidade de TIC, encarregado pelo tratamento dos dados pessoais, gestor de segurança e assessor de controle interno;

c) A implementação consistente das etapas previstas no programa;

d) O desenvolvimento da cultura de privacidade e segurança da informação;

e) A implementação de ações de capacitação nas trilhas de privacidade e segurança da informação;

f) A customização das metodologias e/ou tecnologias disponibilizadas para as realidades dos unidades;

g) E, por fim, o monitoramento contínuo do progresso da implementação do programa e o respectivo reporte de informações para alta administração do órgão.

CONCLUSÃO

38. Dessa forma, ressalta-se a importância da ação coordenada e sinérgica de todos os órgãos do SISP para o alcance dos objetivos previstos na **Estratégia de Governo Digital (EGD) 2020-2022** para a temática da privacidade e segurança da informação, bem como para o cumprimento das orientações exaradas no âmbito do **Acórdão 1.889/2020-TCU-Plenário,** com especial atenção para o processo de identificação, estabelecimento e gerenciamento dos controles internos de privacidade e segurança da informação nos sistemas informacionais críticos apontados pelo Tribunal de Contas da União (TCU).

39. Reforça-se, que tal processo será potencializado pelo engajamento do órgão no **Programa de Privacidade e Segurança da Informação proposto pela SGD/ME**, considerando-se seu caráter transversal, multidisciplinar e orientado para resultados. Conforme se destacou ao longo da presente nota técnica, trata-se de um modelo baseado em 5 (cinco) torres, que terá como enfoque a articulação simultânea das torres de Governança, Pessoas, Metodologia, Tecnologia e Gestão de Maturidade aplicadas aos órgãos e entidades integrantes do SISP detentores dos sistemas informacionais críticos.

40. Por fim, recomenda-se a divulgação da presente nota técnica aos **58 órgãos** integrantes do Sistema de Administração de Recursos de Tecnologia da Informação (SISP), que participaram da auditoria conduzida pelo TCU que resultou na publicação do **Acórdão 1.889/2020-TCU-Plenário.** Nesse contexto, as equipes do Departamento de Governança de Dados e Informações, da Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital, do Ministério da Economia, permanecem à disposição dos órgãos integrantes do SISP para eventuais esclarecimentos.

À consideração do Diretor do Departamento de Governança de Dados e Informações,

Documento assinado eletronicamente

LORIZA ANDRADE VAZ DE MELO

Coordenadora-Geral

De acordo.

À consideração do Secretário de Governo Digital,

Documento assinado eletronicamente

LEONARDO RODRIGO FERREIRA

Diretor

De acordo. Encaminhe-se a presente nota técnica para expedição, em conjunto com o ofício-circular destinado aos órgãos indicados pelo Departamento de Governança de Dados e Informações.

Documento assinado eletronicamente

FERNANDO ANDRÉ COELHO MITKIEWICZ

Secretário de Governo Digital

Documento assinado eletronicamente por **Loriza Andrade Vaz de Melo**, **Coordenador(a)-Geral**, em 24/12/2021, às 17:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Leonardo Rodrigo Ferreira**, **Diretor(a)**, em 24/12/2021, às 17:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fernando André Coelho Mitkiewicz**, **Secretário(a)**, em 24/12/2021, às 18:36, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **14200942** e o código CRC **6F40D4F2**.

Referência: Processo nº 19974.100460/2021-91. SEI nº 14200942