SERVIÇO PÚBLICO FEDERAL
CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA – CONFEA

Processo: CF-00.004680/2022-54

Tipo de Processo: Gestão de TI: Planos e Projetos

Assunto: Política de Backup do Confea

Interessado: Gerência de Tecnologia da Informação, Comitê Gestor de Tecnologia da Informação, Conselho Federal de Engenharia e Agronomia

Relator: Eng. Eletric. Genilson Pavão Almeida

DECISÃO CD Nº 108/2023

Aprova a minuta de Portaria 0692008, que "Institui a Política de Backup e Restauração de Dados Digitais no âmbito do Confea"; e determina providências,

O Conselho Diretor, em sua 4ª Reunião ordinária, realizada no dia 18 de maio de 2023, na Sede do Confea, em Brasília-DF;

Considerando que tratam os presentes autos do Processo 00.004680/2022-54, os quais, de acordo com o Informe 9 (0645419), de 23 de agosto de 2022, foi *criado com o fito de elaboração da Política de Backup do Confea*;

Considerando que, inicialmente, foi juntada aos autos a minuta de Portaria 0692008, firmada pela Chefia de Gabinete - GABI, Superintendência de Estratégia e Gestão - SEG, Superintendência Administrativo e Financeira - SAF, Superintendência de Integração do Sistema - SIS, Gerência de Conhecimento Institucional - GCI e Gerência de Tecnologia da Informação - GTI, consignando na respectiva ementa: Institui a Política de Backup e Restauração de Dados Digitais no âmbito do Confea;

Considerando que por meio da Informação 72 (0692473), de 25 de janeiro de 2023, a Gerência de Tecnologia da Informação - GTI manifestou-se nos seguintes termos:

> 1. Consoante registrado no doc. 0645419, o processo SEI nº 00.004680/2022-54 foi criado com o fito de condução da elaboração da Política de Backup do Confea.
>
> 2. No contexto da transformação digital do Estado Brasileiro, o Governo Federal publicou em 29 de abril de 2020, por meio do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução na Administração Pública.
>
> 2.1. Ela norteia as ações de todos os órgãos federais com o objetivo de transformar o governo pelo Digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.
>
> 3. Hoje, mais do que em qualquer outro momento da história, a tecnologia é utilizada para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.
>
> 4. Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de

saúde; fornecimento de serviços em nuvem; desenvolvimento de comunicações via cabo, *wireless* e/ou satélites; sistemas militares de defesa).

4.1. As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

5. A proteção dessas informações, enquanto agente de tratamento, está designada no **Art.46. da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018 - "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

6. A sua não observância pode impactar diretamente a capacidade de cumprir as missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva e, em última instância, impedir a geração de valor público para o cidadão.

7. Nesse contexto, a Gerência de Tecnologia da Informação tem atuado e buscado adotar as melhores práticas no que tange às contratações de soluções de tecnologia da informação, bem como adequar e atualizar os normativos internos do Confea, sempre em observância às Instruções Normativas e legislações em vigor.

8. Nesse viés, foi proposta a Minuta de Portaria para instituir a Política de Backup e Restauração de Dados Digitais no âmbito do Confea, possuindo como objetivo instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Gerência de Tecnologia da Informação (GTI) e formalmente definidos como de necessária salvaguarda no Conselho Federal de Engenharia e Agronomia - Confea, para se manter a continuidade do negócio.

9. Dentre as motivações e justificativas, citam-se: manutenção da continuidade do negócio do Confea; estabelecimento de mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de perdas por erro humano, ataques externos, catástrofes naturais ou outras ameaças; auxiliar na melhoria da segurança tecnológica no Confea; ser um importante mecanismo de segurança, tanto para o Confea quanto para os usuários; evidenciar o comprometimento da alta administração com vistas a prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação no Confea; estar amparado por documento formal que estabeleça as periodicidades dos backups e os períodos de retenção, bem como os demais aspectos inerentes ao tema.

10. Ainda, quando da elaboração da minuta, foram efetuadas pesquisas nas legislações nacionais, assim como em entidades de renome do setor público, conforme evidenciadas na referência legal contida na minuta, o que, na análise desta Gerência de Tecnologia da Informação, demonstra atendimento da proposta de minuta às diretrizes estabelecidas nas legislações federais.

11. Em virtude da condução do processo SEI nº 01020/2019, que propõe uma Minuta de Portaria da Política de Segurança da Informação do Confea, e visando manter congruência entre as propostas, procurou-se minimamente tratar sobre serviço de backup na referida minuta, de modo que o detalhamento de seus dispositivos se encontram na atual minuta de Política de Backup e Restauração de Dados Digitais.

12. Por fim, registra-se que não existem quaisquer normativos internos no âmbito do Confea que disciplinem a respeito da Política de Backup e Restauração de Dados Digitais, sendo uma iniciativa nova visando atender às legislações federais, bem como às recomendações do TCU e da CGU.

13. Pelo exposto, avaliamos que a proposta sugerida e apresentada cumprirá inicialmente os objetivos quanto à Política de Backup e Restauração de Dados Digitais no âmbito do Confea.

Considerando que por meio do Despacho GTI 0692513, de 25 de janeiro de 2023, a Gerência de Tecnologia da Informação - GTI encaminhou os autos à Superintendência de Estratégia e Gestão - SEG e ao Encarregado de Dados do Confea, nos seguintes termos:

Vimos disponibilizar a Minuta de Portaria (doc. 0692008) que dispõe sobre a instituição da Política de Backup e Restauração de Dados Digitais no âmbito do Confea com o intuito de que seja

apreciada pelo Comitê Gestor de Tecnologia da Informação, em breve, e para que possa ter seu trâmite de aprovação interno.

Através da Informação GTI nº 72/2022 (doc. 0692473), foram apresentadas, dentre outras, as razões e as motivações que justificam a elaboração de uma proposta de normativo, bem como é apresentada uma contextualização do pleito.

Ainda, a Subprocuradoria Consultiva emitiu o Parecer SUCON nº 164/2022 (doc. 0653068) no processo 01020/2019 (Política de Segurança da Informação) quanto a necessidades de adequações e complementações que foram contempladas na atual minuta, ensejando também na necessidade de manifestação do Encarregado de Dados do Confea.

Assim o sendo, solicita-se manifestação técnica do Encarregado da LGPD quanto ao cumprimento da Lei Geral de Proteção de Dados quanto à minuta disponibilizada.

Após, sendo positivo o parecer, o processo será submetido ao Comitê Gestor de Tecnologia da Informação visando sua deliberação e continuidade processual.

Considerando que por meio do Despacho UPD 0711451, de 27 de fevereiro de 2023, o Encarregado de Dados do Confea manifestou-se nos seguintes termos:

Em atenção ao despacho 0692513 seguem manifestações pertinentes em relação à aderência da Política de Backup e Restauração de Dados Digitais no âmbito do Confea proposta, em relação à LGPD.

É importante contextualizar que a Lei 13.709/2018 trata em diversos pontos sobre a necessidade de adoção de meditas técnicas e administrativas para que seja minimizado ou mitigado o risco de incidentes envolvendo dados pessoais e assim garantindo a privacidade do titular cujos dados estão custodiados ao controlador. Embora trate sobre a adoção de medidas técnicas e administrativas, as mesmas não são explícitas na lei, sendo desta forma adotados outros referenciais e boas práticas para a correta adoção de tais medidas, conforme disposto no Art.11 da Minuta de Portaria da referida política 0692008.

Em relação à LGPD, o Art. 6° da LGPD para o tratamento de dados pessoais, as operações devem seguir alguns princípios, dos quais destaco os itens V, VI, VII e VIII por terem vinculo direto com as operações de Backup:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

No âmbito das responsabilidades do Controlado e Operador, destaco da mesma forma os artigos Art. 37 a 40 uma vez que tratam de registros e operações de comprovação de tratamento que se beneficiam da política proposta:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
>
> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
>
> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
>
> Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Nas questões de irregularidade em relação ao tratamento de dados, destaco o Art. 44 que aborda a irregularidade no tratamento de dados pessoais quando não foram aplicadas medidas que garantam a segurança deste tratamento:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> I - o modo pelo qual é realizado;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
>
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

E finalmente, o Art. 46 que aborda mais diretamente a necessidade de adoção das medidas de segurança para a proteção dos dados pessoais e os Art. 47, 48 e 49 que tratam de responsabilidades compartilhadas, informação de eventos à ANPD e aderência as normas regulamentares em adição à própria LGPD:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das

> informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
>
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
>
> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
>
> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Operacionalmente, é importante garantir que os *backups* possam receber as operações de Incluir, Excluir e Ajustar dados dos sistemas em backup ou que estas alterações sejam refletidas nos sistemas conforme estabelece a LGPD nos Art. 17 e 18, assim como em relação ao término do tratamento de dados Art. 16 que prevê a eliminação dos dados.

É pertinente, embora a ANPD ainda não tenha definido regras de compartilhamento internacional de dados, avaliar o contrato com prestadores de serviço que utilizem backup em nuvem para checar se a nuvem usada pela empresa provém de um servidor seguro para que não ocorram violações. Importante avaliar a criptografia dos dados em *backup* visando minimizar efeitos de violação e acesso indevido à estes dados.

As observações operacionais, desde que possíveis em relação aos contratos ativos devem ser seguidas e, no caso de não estarem previstas, apontadas como pontos de melhoria para as próximas contratações, assim como devem constar do mapeamento de riscos para as atividades de *backup*.

Deve-se ainda ressaltar que a eliminação dos dados é parte do ciclo de vida dos dados, é uma etapa que deve ocorrer para a eficiência do processamento, armazenamento e da localização de outras informações. Consoante ao disposto no art. 27 da minuta proposta, para eliminação deve ser considerado o prazo de retenção e o disposto na Tabela de Temporalidade em vigor. A eliminação de dados e informações públicas, bem como de documentos onde podem estar, obedece à legislação específica, que deve ser observada para ocorrência, das quais citamos a Lei nº

8.159/1991, Decreto nº 10.148/2019 e a Resoluções nº 40 e 44 do Conselho Nacional de Arquivos (CONARQ).

Para a política em questão, do ponto de vista das exigências em relação à Lei 13.709/2018, não existem adequações administrativas necessárias.

Considerando que por meio do Despacho GTI 0735274, de 22 de março de 2023, a Gerência de Tecnologia da Informação - GTI submeteu os autos ***aos membros do Comitê Gestor de Tecnologia da Informação disciplinado pela Portaria nº 190/2014 - doc. 0294139***:

Sr. Luiz Antônio Rossafa, Chefe de Gabinete - GABI

Sr. Osmar Barros Júnior, Superintendente de Integração do Sistema - SIS

Sr. Renato Gonçalves Barros, Superintendente de Estratégia e Gestão - SEG

Sr. Jadir José Alberti, Superintendente Administrativo e Financeiro - SAF

Sr. Renato Gonçalves Barros, Gerente de Planejamento e Gestão - GPG

Sr. Rabah Mohamed Awadalla Rabah Abdelgawad, Gerente de Conhecimento Institucional - GCI

Em breve histórico processual, na reunião ordinária do Comitê Gestor de Tecnologia da Informação em julho de 2022 (doc. 0620028), os seguintes assuntos para conhecimento foram tratados: PDTI - Plano Diretor de Tecnologia da Informação; Política de backup; Atualização da Portaria do CGTI; e Política de Classificação de Documentos.

O presente processo versa sobre a elaboração da Minuta de Portaria para "Instituir a Política de Backup e Restauração de Dados Digitais no âmbito do Confea".

Apoiado no Parecer SUCON nº 164/2022 (doc. 0653068) quanto ao processo da Política de Segurança da Informação (SEI 01020/2019), todas as recomendações ora efetuadas foram avaliadas e aplicadas neste processo naquilo que foi cabível.

Assim, dentre os principais documentos aqui constantes, citam-se:

1. Informação GTI nº 72/2022 (doc. 0692473).

2. Despacho UPD (doc. 0711451).

3. Minuta de Portaria (doc. 0692008).

Cumpridas todas as etapas iniciais, após alinhamento entre o gestor de tecnologia da informação e o superintendente de estratégia e gestão, decidiu-se encaminhar o presente processo às unidades dos membros do CGTI para que conheçam a Minuta de Portaria (doc. 0692008), sugiram eventuais alterações ou, no caso de concordância, promovam sua assinatura através do bloco de assinatura nº 12198 em analogia ao que fora efetuado em momento anterior através da Súmula CGTI (doc. 0625361), porém, para o presente momento, assinatura na própria Minuta de Portaria (doc. 0691528).

Tal ato constituirá na aprovação da referida minuta pelo respectivo membro e, uma vez aprovada e assinada a Minuta de Portaria (doc. 0691528) pelos membros do CGTI, o processo será remetido à Procuradoria Jurídica para análise jurídica.

Pelo exposto, a Gerência de Tecnologia da Informação e a Superintendência de Estratégia e Gestão se encontram à disposição para quaisquer esclarecimentos.

Considerando que por meio do Despacho GPG 0735454, de 23 de março de 2023, a Gerência de Planejamento e Gestão - GPG manifestou-se nos seguintes termos:

Considerando o despacho GTI (SEI 0735274) e demais documentos, informo que efetuei a assinatura como superintendente de estratégia e gestão na minuta de portaria (SEI 0692008), sendo que o SEI não permite nova assinatura no mesmo documento.
De qualquer forma, como gerente da gerência de planejamento e gestão interino, aprovo a minuta de portaria (SEI 0692008).

Considerando que por meio do Despacho CGTI 0737528, de 28 de março de 2023, a Gerência de Tecnologia da Informação - GTI encaminhou os autos à Superintendência de Estratégia e Gestão - SEG, nos seguintes termos:

> Encaminha-se o presente processo visando apreciação pela Procuradoria Jurídica quanto à Minuta de Portaria que "Institui a Política de Backup e Restauração de Dados Digitais no âmbito do Confea" constante no doc. 0692008.
>
> Embasado no processo que trata a Minuta da Política de Segurança da Informação (SEI 01020/2019) e que consta o Parecer SUCON nº 164/2022 (doc. 0653068), foram promovidas as complementações e adequações processuais conforme dispostas nos seguintes documentos: Informação GTI nº 72/2022 (doc. 0692473), Despacho GTI (doc nº 0692513) e Despacho UPD (doc. 0711451).
>
> Ademais, registra-se que a referida Minuta de Portaria foi apreciada pelo Comitê Gestor de Tecnologia da Informação - CGTI, através de sua disponibilização aos membros (doc. 0735274), tendo sido assinada por todos e se encontrando apta à apreciação jurídica.

Considerando que por meio do Despacho SEG 0737614, de 28 de março de 2023, a Superintendência de Estratégia e Gestão - SEG encaminhou os autos à Chefia de Gabinete - GABI, nos seguintes termos:

> Considerando a informação 72 (SEI 0692473), despacho CGTI - Comitê Gestor de Tecnologia da Informação (SEI 0737528), minuta de portaria (SEI 0692008) e demais documentos, encaminho para as tratativas cabíveis.

Considerando que por meio do Despacho GABI 0738655, de 29 de março de 2023, a Chefia de Gabinete - GABI encaminhou os autos à Procuradoria Jurídica - PROJ, nos seguintes termos:

> Trata-se da Minuta de Portaria que "Institui a Política de Backup e Restauração de Dados Digitais no âmbito do Confea" constante no doc 0692008.
>
> Em que pese alguns ajustes de forma que necessitam ser realizados na respectiva minuta, encaminho o processo para análise e parecer jurídico a fim de subsidiar decisão do Conselho Diretor.

Considerando que por meio do Parecer 55 (0748197), de 20 de abril de 2023, a Subprocuradoria Consultiva manifestou-se nos seguintes termos:

> **I - RELATÓRIO**
>
> 1. Trata-se de solicitação para que esta Procuradoria Jurídica proceda à análise da Política de Backup do Confea, constante na Minuta de Portaria anexa (0692008).
>
> 2. A norma está relacionada com a Política de Segurança da Informação que é objeto do Processo 01020/2019.
>
> 3. A Gerência de Tecnologia da Informação realizou análise técnica, por meio da Informação GTI nº 72/2022 (0692473), sendo favorável à aprovação do texto.
>
> 4. A área de proteção de dados analisou o texto sob a ótica da Lei Geral de Proteção de Dados (Lei nº 13.709, de 2018), conforme Despacho UPD 0711451, se manifestando favoravelmente.
>
> 5. É o que importa relatar.
>
> **II - ANÁLISE JURÍDICA**

6. Inicialmente, cumpre-nos salientar que a presente manifestação jurídica toma por base, exclusivamente, os elementos que constam, até a presente data, nos autos do processo em epígrafe, valendo ressaltar que não cabe a esta unidade jurídica adentrar nos aspectos técnicos, econômicos e operacionais, nem no juízo de oportunidade e conveniência da instituição do presente regulamento.

7. A proposta está devidamente motivada, integrando o rol de normas que precisam ser alteradas para aperfeiçoar a política de tecnologia da informação, conforme justificativa constante na Informação GTI nº 72/2022 (0692473), que assevera o seguinte:

> 1. Consoante registrado no doc. 0645419, o processo SEI nº 00.004680/2022-54 foi criado com o fito de condução da elaboração da Política de Backup do Confea.
>
> 2. No contexto da transformação digital do Estado Brasileiro, o Governo Federal publicou em 29 de abril de 2020, por meio do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução na Administração Pública.
>
> 2.1. Ela norteia as ações de todos os órgãos federais com o objetivo de transformar o governo pelo Digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.
>
> 3. Hoje, mais do que em qualquer outro momento da história, a tecnologia é utilizada para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.
>
> 4. Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvimento de comunicações via cabo, *wireless* e/ou satélites; sistemas militares de defesa).
>
> 4.1. As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.
>
> 5. A proteção dessas informações, enquanto agente de tratamento, está designada no **Art.46. da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018 - "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
>
> 6. A sua não observância pode impactar diretamente a capacidade de cumprir as missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva e, em última instância, impedir a geração de valor público para o cidadão.
>
> 7. Nesse contexto, a Gerência de Tecnologia da Informação tem atuado e buscado adotar as melhores práticas no que tange às contratações de soluções de tecnologia da informação, bem como adequar e atualizar os normativos internos do Confea, sempre em observância às Instruções Normativas e legislações em vigor.
>
> 8. Nesse viés, foi proposta a Minuta de Portaria para instituir a Política de Backup e Restauração de Dados Digitais no âmbito do Confea, possuindo como objetivo instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Gerência de Tecnologia da Informação (GTI) e formalmente definidos como de necessária salvaguarda no Conselho Federal de Engenharia e Agronomia - Confea, para se manter a continuidade do negócio.
>
> 8.9. Dentre as motivações e justificativas, citam-se: manutenção da continuidade do negócio do Confea; estabelecimento de mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de perdas por erro humano, ataques

externos, catástrofes naturais ou outras ameaças; auxiliar na melhoria da segurança tecnológica no Confea; ser um importante mecanismo de segurança, tanto para o Confea quanto para os usuários; evidenciar o comprometimento da alta administração com vistas a prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação no Confea; estar amparado por documento formal que estabeleça as periodicidades dos backups e os períodos de retenção, bem como os demais aspectos inerentes ao tema.

10. Ainda, quando da elaboração da minuta, foram efetuadas pesquisas nas legislações nacionais, assim como em entidades de renome do setor público, conforme evidenciadas na referência legal contida na minuta, o que, na análise desta Gerência de Tecnologia da Informação, demonstra atendimento da proposta de minuta às diretrizes estabelecidas nas legislações federais.

11. Em virtude da condução do processo SEI nº 01020/2019, que propõe uma Minuta de Portaria da Política de Segurança da Informação do Confea, e visando manter congruência entre as propostas, procurou-se minimamente tratar sobre serviço de backup na referida minuta, de modo que o detalhamento de seus dispositivos se encontram na atual minuta de Política de Backup e Restauração de Dados Digitais.

12. Por fim, registra-se que não existem quaisquer normativos internos no âmbito do Confea que disciplinem a respeito da Política de Backup e Restauração de Dados Digitais, sendo uma iniciativa nova visando atender às legislações federais, bem como às recomendações do TCU e da CGU.

13. Pelo exposto, avaliamos que a proposta sugerida e apresentada cumprirá inicialmente os objetivos quanto à Política de Backup e Restauração de Dados Digitais no âmbito do Confea.

8. Quanto ao texto apresentado na Minuta de Portaria anexa (0692008), é preciso ressaltar que a regulamentação em questão está em consonância com a Política de Segurança da Informação que é objeto do Processo 01020/2019, onde consta o seguinte:

Art. 9º A unidade organizacional responsável pela tecnologia da informação no Confea possui os seguintes deveres específicos:

(...)

VI - administrar, proteger e testar cópias de segurança dos programas e dados relacionados aos processos do Confea consoante política de backup definida;

(...)

Art. 34. Arquivos imprescindíveis para as atividades dos usuários deverão ser salvos em *drives* de rede do Conselho, como o servidor de arquivos e o *OneDrive*, quando para arquivos em transferência e públicos, ou nas pastas específicas de cada unidade organizacional, com o devido acesso autorizado e restrito aos envolvidos.

Parágrafo único. Os arquivos mencionados no caput, se gravados apenas localmente nos dispositivos eletrônicos (por exemplo, no drive C: de computadores), não terão garantia de *backup* e poderão ser perdidos caso ocorram falhas no equipamento, pois não é responsabilidade da unidade organizacional responsável pela tecnologia da informação realizar *backup* de documentos particulares, e até mesmo corporativos, que estiverem armazenados localmente.

(...)

Art. 51. O acesso a softwares *peer-to-peer* ou *storage backup* (*eMule, BitTorrent, Google Drive, Dropbox* e afins) não é permitido, salvo quando autorizado pelo gestor da unidade organizacional responsável pela tecnologia da informação.

Art. 52. O softwares *de storage backup,* colaboração e compartilhamento em nuvem licenciado e permitido para uso corporativo é o *OneDrive,* da *Microsoft,* que deve ser utilizado mediante uso de login e senha de rede.

Parágrafo único. Serviços de *streaming* (rádios on-line, canais de *broadcast* e afins) são permitidos a determinadas unidades organizacionais.

(...)

> Art. 66. Os procedimentos próprios relacionados ao serviço de *backup* (cópia de segurança) são previstos em normativo próprio, consideradas as seguintes diretrizes gerais:
>
> I - o serviço de *backup* deve ser automatizado por sistemas informacionais próprios, com execuções agendadas;
>
> II - a solução de *backup* deve ser atualizada, haja vista, por exemplo, novas versões, ciclo de vida, garantia, melhorias e atualizações de correção;
>
> III - a administração das mídias de *backup* deve ser contemplada em normas complementares sobre o serviço, para garantir a segurança e a integridade do processo;
>
> IV - é recomendável a previsão, em orçamento anual, de aprimoramento das mídias de *backup* - em virtude do desgaste ordinário, bem como deve-se manter estoque constante de mídias para qualquer uso emergencial;
>
> V - as mídias de *backups* históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofre;
>
> VI - os *backups* críticos ao bom funcionamento do Confea e respectiva carta de serviços exigem regra de retenção especial, a ser prevista em procedimentos específicos e de acordo com as normas de classificação de informações públicas, seguindo, ainda, determinações fiscais e legais existentes no país; e
>
> VII - a execução de rotinas de *backup* e *restore* deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

9. Ademais, o texto atende as diretrizes fixadas no Decreto nº 10.332, de 2020, especialmente no que concerne à Estratégia de Governo Digital e, especialmente, os cuidados com a segurança e o sigilo de dados, da Lei Geral de Proteção de Dados (Lei nº 13.709, de 2018).

10. A propósito do assunto, a unidade responsável pela cumprimento da Lei Geral de Proteção de Dados (Lei nº 13.709, de 2018), assevera a compatibilidade do texto com as regras gerais de proteção de dados, conforme Despacho UPD 0711451, que destaca o seguinte:

> Operacionalmente, é importante garantir que os *backups* possam receber as operações de Incluir, Excluir e Ajustar dados dos sistemas em backup ou que estas alterações sejam refletidas nos sistemas conforme estabelece a LGPD nos Art. 17 e 18, assim como em relação ao término do tratamento de dados Art. 16 que prevê a eliminação dos dados.
>
> É pertinente, embora a ANPD ainda não tenha definido regras de compartilhamento internacional de dados, avaliar o contrato com prestadores de serviço que utilizem backup em nuvem para checar se a nuvem usada pela empresa provém de um servidor seguro para que não ocorram violações. Importante avaliar a criptografia dos dados em *backup* visando minimizar efeitos de violação e acesso indevido à estes dados.
>
> As observações operacionais, desde que possíveis em relação aos contratos ativos devem ser seguidas e, no caso de não estarem previstas, apontadas como pontos de melhoria para as próximas contratações, assim como devem constar do mapeamento de riscos para as atividades de *backup*.
>
> Deve-se ainda ressaltar que a eliminação dos dados é parte do ciclo de vida dos dados, é uma etapa que deve ocorrer para a eficiência do processamento, armazenamento e da localização de outras informações. Consoante ao disposto no art. 27 da minuta proposta, para eliminação deve ser considerado o prazo de retenção e o disposto na Tabela de Temporalidade em vigor. A eliminação de dados e informações públicas, bem como de documentos onde podem estar, obedece à legislação específica, que deve ser observada para ocorrência, das quais citamos a Lei nº 8.159/1991, Decreto nº 10.148/2019 e a Resoluções nº 40 e 44 do Conselho Nacional de Arquivos (CONARQ).
>
> Para a política em questão, do ponto de vista das exigências em relação à Lei 13.709/2018, não existem adequações administrativas necessárias.

11. Assim, diante da análise técnica da Gerência de Tecnologia da Informação e do setor responsável pela proteção de dados, infere-se que os aspectos técnicos necessários à segurança da

informação estão contemplados na minuta apresentada, não cabendo à Procuradoria Jurídica se imiscuir nessa seara.

III - CONCLUSÃO

12. Ante o exposto, considerando os elementos que constam nos autos até o momento, ressalvando-se os aspectos de conveniência e oportunidade não sujeitos ao crivo da presente análise, conclui-se, do ponto de vista estritamente jurídico, em sede de controle prévio de juridicidade, pela legalidade da Política de Backup do Confea, constante na Minuta de Portaria anexa (0692008), motivo pelo qual não se verifica óbice, nesse aspecto, para o prosseguimento do feito, visando a aprovação do documento.

Considerando que, de acordo com o disposto no art. 57 da Resolução nº 1.015, de 30 de junho de 2006, o Conselho Diretor – CD tem por finalidade auxiliar o Plenário na gestão do Confea;

Considerando que os incisos XI e XII do art. 63 da supracitada Resolução estabelecem que compete ao Conselho Diretor - CD:

(...)

XI – apreciar e decidir sobre o funcionamento das unidades organizacionais do Confea, bem como lhes propor modificações;

XII – apreciar e decidir sobre a estrutura organizacional e as rotinas administrativas do Confea propostas pelo presidente;

(...)

Considerando que por meio do Despacho CD 0754713 o Presidente do Confea acolheu a minuta de Portaria 0692008, apresentando-a como Proposta desta Presidência do Confea, à luz do disposto nos incisos XI e XII do art. 63 da Resolução nº 1.015, de 30 de junho de 2006;

DECIDIU, por unanimidade:

1) Aprovar a minuta de Portaria 0692008, que "Institui a Política de Backup e Restauração de Dados Digitais no âmbito do Confea";

2) Encaminhar os autos à Chefia de Gabinete - GABI, para as providências decorrentes no tocante à revisão gramatical, eventuais ajustes de forma, numeração, coleta de assinaturas, comunicações e encaminhamentos pertinentes,

Presidiu a sessão o Eng. Civ. **Joel Krüger**. Presentes o Vice-Presidente, Eng. Eletric. **Evânio Ramos Nicoleit** e os Diretores Eng. Agr. **Cândido Carnaúba Mota**, Eng. Eletric. **Genilson Pavão Almeida**, Eng. Eletric. **Jorge Luiz Bitencourt da Rocha**, Geol. **Mário Cavalcanti de Albuquerque** e o Eng. Civ. **Neemias Machado Barbosa**.

Cientifique-se e cumpra-se.

Documento assinado eletronicamente por **Joel Krüger**, **Presidente**, em 22/05/2023, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.