CONSELHO REGIONAL DE CONTABILIDADE DE GOIÁS

RESOLUÇÃO CRCGO Nº 511, DE 28 DE JANEIRO DE 2025

Dispõe, ad-referendum, sobre a Política de Armazenamento de Dados, Documentos e Informações do Conselho Regional de Contabilidade de Goiás.

O CONSELHO REGIONAL DE CONTABILIDADE DE GOIÁS, no uso de suas atribuições legais e regimentais, resolve:

Art. 1º Fica instituída a Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade de Goiás (CRCGO), nos termos do Anexo desta Resolução.

Parágrafo único. Todos os instrumentos normativos gerados a partir da Política de Armazenamento de Dados, Documentos e Arquivos do Conselho Regional de Contabilidade de Goiás (CRCGO) são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos.

Art. 2º A Política de Armazenamento de Dados, Documentos e Arquivos do Conselho Regional de Contabilidade de Goiás aplica-se a todos os conselheiros, empregados, estagiários, prestadores de serviços e, quando cabível, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCGO e que tenham acesso a qualquer documento, arquivo e meio de informação e comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Art. 3º A íntegra da Política de Armazenamento de Dados, Documentos e Arquivos do Conselho Regional de Contabilidade de Goiás será disponibilizada no portal e na intranet do CRCGO.

Art. 4º Esta Resolução revoga a Resolução CRCGO nº 455, de 11 de outubro de 2022.

Art. 5º Esta Resolução entra em vigor na data de sua assinatura.

CONTADORA SUCENA HUMMEL

Presidente

ANEXO

POLÍTICA DE ARMAZENAMENTO DE DADOS, DOCUMENTOS E ARQUIVOS (PADDA) DO CRCGO

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

Das Premissas

Art. 1º As normas desta Política aplicam-se aos conselheiros, empregados, colaboradores, bem como a quaisquer pessoas que tenham acesso a dados, arquivos e documentos do CRCGO.

Art. 2º A Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) tem por objetivo:

I – garantir condições para que os conselheiros, empregados, colaboradores e, quando cabível, terceiros e quaisquer outras pessoas que prestem serviços ao CRCGO sejam orientados sobre a existência e a utilização dos instrumentos normativos, procedimentos e controles de uso e armazenamento adotados pelo CRCGO;

II – assegurar as condições adequadas ao pleno acesso a documentos digitais e não digitais, pelo prazo institucionalmente estabelecido;

III – assegurar, permanentemente, a autenticidade dos documentos digitais e não digitais;

IV – implantar repositório institucional próprio para a preservação digital;

V – contribuir para a redução do risco em segurança da informação; e

VI – manter os documentos em ambiente físico ou eletrônico seguro e a implementação de estratégias de preservação desses documentos desde sua produção e durante o período de guarda definido.

Art. 3º As diretrizes desta Política visam assegurar que dados, documentos e arquivos digitais e não digitais de uso sensível e/ou sigiloso sejam removidos do espaço de trabalho do usuário e guardados quando não estiverem em uso ou em períodos de ausência do usuário.

Art. 4º As diretrizes desta Política visam assegurar que dados, documentos e arquivos de uso sensível e/ou sigiloso digitais sejam armazenados de modo a garantir a sua recuperação, integridade e autenticidade, para que possam servir de fonte de prova e informação.

Seção II

Dos Objetivos

Art. 5º Esta Política tem o objetivo de estabelecer as melhores práticas para o manuseio e o

armazenamento de documentos não digitais e arquivos digitais do CRCGO.

Parágrafo único. A PADDA está alinhada às estratégias institucionais, à política de governança, à gestão de riscos e aos normativos que regem a matéria.

Art. 6º A PADDA trata do uso e do armazenamento de dados, arquivos e documentos no âmbito do CRCGO, em todo o seu ciclo de vida, e objetiva a continuidade de seus processos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação armazenadas no âmbito do CRCGO.

Art. 7º Para a segurança do uso e do armazenamento da informação no CRCGO, serão rigorosamente observados o compromisso institucional com a proteção das informações de sua propriedade e/ou sob sua guarda, a participação e o cumprimento por todos os colaboradores em todo o processo e o disposto neste normativo, nas disposições constitucionais, legais e regimentais vigentes.

Seção III

Dos Princípios e Diretrizes

Art. 8º A PADDA do CRCGO orienta-se pelos seguintes princípios e diretrizes:

I – o CRCGO deve desempenhar o papel de um custodiador de confiança;

II – o Conselho Regional de Contabilidade de Goiás é responsável pela custódia física e legal dos documentos digitais e não digitais a ele recolhidos e inseridos nos repositórios do CRCGO como um custodiador de confiança, a PADDA deve possibilitar que o CRCGO possa:

a) atuar com neutralidade, ou seja, demonstrar que não tem razões para alterar os documentos sob sua custódia e que não permitirá que outros alterem esses documentos, acidental ou propositalmente;

b) implantar um sistema de uso, armazenamento e preservação confiável, capaz de garantir autenticidade dos documentos em conformidade com a legislação arquivística brasileira vigente;

III – garantir a preservação de todos os componentes digitais e não digitais dos documentos produzidos, recebidos e armazenados, de modo a permitir a apresentação desses documentos no futuro;

IV – o grau de sigilo e a restrição de acesso à informação sensível relacionados aos documentos produzidos, recebidos e armazenados têm que ser identificados explicitamente e garantidos pelo CRCGO;

V – gerenciar, no repositório, a permissão de acesso de documentos com grau de sigilo e/ou que registrem informação sensível, de acordo com legislação vigente e as normas de controle de acesso definidas no âmbito do CRCGO. Essas restrições devem ser registradas em metadados e procedimentos de acesso às áreas de armazenamento de dados, documentos e arquivos do CRCGO; e

VI – garantir o acesso a informações necessárias ao exercício de direitos.

Seção IV

Do Repositório para o Armazenamento e a Preservação Digital

Art. 9º O Conselho Regional de Contabilidade de Goiás deverá criar e manter repositório arquivístico digital confiável institucional dedicado à preservação digital.

§ 1º O repositório de preservação digital compreende tanto o software como também o hardware correspondente.

§ 2º O repositório de preservação digital utilizará, preferencialmente, padrões abertos.

§ 3º O repositório de preservação digital deverá contemplar a norma brasileira NBR 15.472, de 9 de abril de 2007, em seu modelo de referência para um sistema aberto de arquivamento de informação (SAAI).

§ 4º O repositório de preservação digital deverá contemplar a Resolução Conarq nº 51, de 25 de agosto

de 2023, e alterações posteriores, que dispõem sobre as Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis.

§ 5º As ações necessárias à atualização tecnológica do repositório de preservação digital integrarão o Plano de Trabalho da Coordenadoria de Gestão e Tecnologia da Informação do CRCGO ou outra unidade organizacional equivalente.

Art. 10. Somente serão encaminhados e aceitos no repositório de preservação digital os documentos digitais consolidados, em sua versão final, e que tenham sido submetidos à avaliação documental.

§ 1º Os documentos digitais de guarda permanente deverão, obrigatoriamente, ser encaminhados ao repositório e terão prioridade de recursos em relação aos demais.

§ 2º Os documentos digitais que não sejam de guarda permanente serão encaminhados ao repositório de acordo com a necessidade de adoção de ações específicas de preservação digital, para mantê-los pelos prazos estabelecidos em seu processo de avaliação.

Art. 11. Os documentos digitais consolidados aceitos no repositório de preservação digital deverão atender aos requisitos de acesso e recuperação integral de seu conteúdo, devendo ser compreensíveis independentemente em relação aos sistemas que os produziram.

Art. 12. Ao conteúdo de cada documento digital enviado ao repositório de preservação digital deverá ser acrescido um pacote de informações que identifique sua proveniência, contexto, referência e fixidez.

§ 1º As informações necessárias para criar o pacote de informações são parte dos requisitos de preservação digital.

§ 2º Os pacotes de informações deverão possuir descritores que os identifiquem claramente em relação aos demais.

Art. 13. Os documentos digitais que forem aceitos no repositório de preservação, bem como seus respectivos pacotes de informações, deverão ter seu histórico de processamento preservado indefinidamente.

Parágrafo único. Nos procedimentos de migração de documentos digitais, poderão ser mantidas versões anteriores dos documentos digitais por razões históricas.

Art. 14. As unidades organizacionais responsáveis pela gestão da preservação digital passam a ter controle sobre os documentos recebidos no repositório de preservação.

Seção V

Da Abrangência

Art. 15. O disposto neste instrumento aplicar-se-á a todos os conselheiros, empregados e colaboradores que prestem serviços ao CRCGO e que tenham acesso a qualquer informação ou comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação.

CAPÍTULO II

DOS CONCEITOS E DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Seção I

Dos Conceitos e Definições

Art. 16. Para os efeitos desta Política de Armazenamento de Dados, Documentos e Arquivos entende-se por:

I – acessibilidade: facilidade no acesso ao conteúdo e ao significado de um objeto digital;

II – armazenamento: guarda de documentos arquivísticos em local apropriado;

III – armazenamento digital: guarda de documentos digitais em dispositivos de memória não volátil;

IV – arquivamento: sequência de operações intelectuais e físicas que visam à guarda ordenada de documentos, é ainda a ação pela qual uma autoridade determina a guarda de um documento, cessada a sua tramitação.;

V – arquivo digital: conjunto de bits que formam uma unidade lógica interpretável por um programa de computador e armazenada em suporte apropriado;

VI – ativo de informação: qualquer dispositivo de software ou hardware que agrega valor ao negócio e compõe a infraestrutura de rede de dados do CRCGO, assim como também os locais onde se encontram esses dispositivos, gestão do pessoal que a eles possuem acesso, além dos processos envolvidos na gestão e na operacionalização dos ativos de informação;

VII – banco de dados: um sistema de armazenamento de dados, ou seja, um conjunto de registros que têm como objetivo organizar e guardar as informações;

VIII – cadeia de custódia ininterrupta: linha contínua de custodiadores de documentos arquivísticos (desde o seu produtor até o seu legitimo sucessor) pela qual se assegura que esses documentos são os mesmos desde o início, não sofreram nenhum processo de alteração e, portanto, são autênticos;

IX – computação em nuvem: modelo computacional que permite acesso, por demanda e independentemente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

X – confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

XI – controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso do usuário;

XII – cópia de segurança: guarda de dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade;

XIII – custódia: responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade;

XIV – custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, recepção, produção, reprodução, utilização, acesso, transporte, transmissão e distribuição;

XV – disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado;

XVI – dispositivos móveis: equipamentos portáteis, dotados de capacidade computacional e dispositivos removíveis de memória para armazenamento, entre eles, notebooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

XVII – documento arquivístico: documento produzido ou recebido no curso de uma atividade prática como instrumento ou resultado dessa atividade, retido para ação ou referência;

XVIII – documento digital: informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional;

XIX – documento não digital: documento que se apresenta em suporte, formato e codificação diferente dos digitais, tais como: documentos em papel, documentos em películas e documentos eletrônicos analógicos;

XX – fidedignidade: credibilidade de um documento arquivístico como uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;

XXI – gestão de segurança da informação: ações e métodos que visam à integração das atividades de

gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

XXII – incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

XXIII – informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

XXIV – integridade: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencionais ou acidentais, em seu estado e atividades;

XXV – metadados: dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

XXVI – Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

XXVII – preservação: prevenção da deterioração e danos em documentos, documentos por meio de adequado controle ambiental e/ou tratamento físico e/ou químico;

XXVIII – preservação digital: conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, a fim de garantir o acesso e a interpretação de documentos digitais pelo tempo que for necessário;

XXIX – público-alvo: conjunto de usuários internos e externos atendidos pela equipe de tratamento e resposta a incidentes;

XXX – recurso criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXXI – repositório arquivístico digital: repositório digital que armazena e gerencia documentos arquivísticos, seja nas idades corrente e intermediária, seja na idade permanente;

XXXII – repositório arquivístico digital confiável: é o repositório que deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável;

XXXIII – repositório digital: plataforma tecnológica que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos;

XXXIV – repositório digital confiável: é um repositório digital que é capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário;

XXXV – risco: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

XXXVI – segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

XXXVII – sistema de armazenamento: solução tecnológica de hardware e software utilizada para o armazenamento de dados;

XXXVIII – tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXXIX – unidade gestora de segurança da informação: é a unidade responsável pela gestão de segurança da informação no CRCGO;

XL – unidade organizacional: unidade em que está lotado o empregado, assessor, terceirizado, estagiário

ou aprendiz;

XLI – usuários: pessoa física ou jurídica que opera algum sistema informatizado do Conselho Regional de Contabilidade de Goiás; e

XLII – vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças.

Seção II

Da Classificação das Informações

Art. 17. A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrange informações provenientes dos serviços essenciais de tecnologia da informação e de gestão documental do CRCGO.

Parágrafo único. As informações devem ser classificadas de forma a permitir tratamento diferenciado de acordo com o seu grau de importância, criticidade, sensibilidade e em conformidade com requisitos legais.

Art. 18. As informações devem ser classificadas e identificadas em conformidade com a Política de Classificação do CRCGO vigente.

CAPÍTULO III

DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I

Das Competências

Art. 19. À Coordenadoria de Gestão de TI, ao Departamento de Suporte e Infraestrutura e ao Departamento de Segurança da Informação competem:

I – promover e estruturar a preservação e o armazenamento dos documentos arquivísticos digitais, nas fases corrente, intermediária e permanente, que devem estar associadas a um repositório arquivístico digital confiável. Os arquivos digitais devem dispor de repositórios arquivísticos digitais confiáveis para a gestão, a preservação e o acesso a documentos digitais, em conformidade com a legislação arquivística vigente;

II – elaborar plano de ação para disponibilizar os repositórios digitais confiáveis para a gestão, a preservação e o acesso a documentos digitais, de acordo com as diretrizes previstas na Resolução nº 51, de 25 de agosto de 2023, do Conselho Nacional de Arquivos (Conarq); e

III – implantar os parâmetros para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade, identidade, integridade, confidencialidade, disponibilidade, o acesso e a preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos de tempo ou, até mesmo, permanentemente;

Seção II

Das Responsabilidades

Subseção I

Dos Usuários

Art. 20. Os usuários e quaisquer outras pessoas que prestem serviços ao CRCGO e tenham acesso ao

ambiente de uso e armazenamento de dados, documentos e arquivos digitais e não digitais do Conselho, têm as seguintes responsabilidades:

I – ter pleno conhecimento e cumprir fielmente esta Política, as normas e os procedimentos de uso e armazenamento do CRCGO;

II – solicitar esclarecimentos à Comissão de Implantação da Lei Geral de Proteção de Dados, em caso de dúvidas relacionadas à esta Política;

III – gerenciar os dados, documentos e arquivos digitais e não digitais sob sua responsabilidade e garantir que os dados, documentos e arquivos não digitais ou digitais, equipamentos e recursos tecnológicos à sua disposição permaneçam seguros;

IV – armazenar documentos não digitais em ambientes seguros, não devendo permanecer sobre a mesa de trabalho do usuário quando não estiver em uso, ou em locais onde pessoas não autorizadas tenham acesso ao seu conteúdo;

V – remover do espaço de trabalho dados, informações, documentos e arquivos sensíveis e/ou sigilosos quando ausente e ao final do dia de trabalho;

VI – manter trancados armários com documentos sensíveis e/ou sigilosos quando não estiverem em uso;

VII – manter em sigilo as chaves/senhas/credenciais usadas para acesso a informações, documentos e arquivos sensíveis;

VIII – evitar a impressão de documentos que contenham informações sensíveis e/ou sigilosas. Em caso de impressão, remover o documento imediatamente da impressora;

IX – restituir prontamente os documentos recebidos por empréstimo de outras unidades, quando não forem mais necessários;

X – utilizar recursos de criptografia e guardar em locais seguros de armazenamento documentos que contenham informações sensíveis e/ou sigilosas;

XI – salvar e armazenar dentro da pasta ou unidade lógica específicas, documentos que contenham dados pessoais;

XII – zelar pela custódia de dados e informações institucionais e evitar o salvamento de conteúdos e informações pessoais em máquinas e espaço físico do Conselho;

XIII – tratar terminais particulares como se institucionais fossem;

XIV – garantir que todas as informações não digitais e digitais sejam mantidas e armazenadas em local seguro quando não estiverem em uso;

XV – armazenar os documentos que contenham dados pessoais somente pelo período necessário ao seu uso ou cumprimento do seu dever legal e dos prazos de guarda e locais indicados na Tabela de Temporalidade de Documentos utilizada no CRCGO, em conformidade com a legislação vigente;

XVI – seguir os procedimentos e a legislação vigente para a eliminação de documentos digitais e não digitais do CRCGO; e

XVII – estar ciente de que toda informação digital ou não digital armazenada, processada e transmitida no ambiente computacional ou físico do CRCGO pode ser auditada.

Subseção II

Do Custodiante

Art. 21. Ao custodiante da Informação cabem as seguintes responsabilidades:

I – cumprir e zelar pela observância integral das diretrizes desta Política e demais normas e procedimentos decorrentes;

II – zelar pela disponibilidade, integridade e confidencialidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta Política e demais normas e procedimentos referentes ao uso e armazenamento de dados, documentos e arquivos;

III – participar de capacitação e treinamento em procedimentos de uso e armazenamento de dados, documentos e arquivos, quando convocado;

IV – proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada; e

V – comunicar prontamente ao seu gestor imediato e ao Comitê de Segurança da Informação qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, integridade e confidencialidade das informações armazenadas.

Subseção III

Dos Gestores das Unidades Organizacionais

Art. 22. Os gestores das unidades organizacionais são responsáveis por:

I – ter postura exemplar em relação ao uso e armazenamento de dados, documentos e arquivos para servir como modelo de conduta para os colaboradores sob sua gestão;

II – cumprir e fazer cumprir esta Política;

III – adotar os procedimentos necessários sempre que identificar descumprimentos da Política de Armazenamento de Dados, Documentos e Informações.

CAPÍTULO IV

DA DIVULGAÇÃO E ATUALIZAÇÃO

Art. 23. Esta Política e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários e disponibilizadas no portal e na intranet do CRCGO, sendo consideradas um documento de relevante interesse público.

Art. 24. Esta Política de Armazenamento de Dados, Documentos e Arquivos deverá ser revisada sempre que se fizer necessário.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 25. Os casos omissos desta Política serão resolvidos pelo Comitê Gestor de Privacidade e Proteção de Dados do CRCGO.

Art. 26. Esta Resolução entrará em vigor na data de sua assinatura.