INSTRUÇÃO NORMATIVA N° 9/2025/SEA

Dispõe sobre a gestão de documentos digitais utilizados para a tramitação, armazenamento e comunicação de informações no âmbito dos órgãos e entidades da Administração Pública Estadual, com o objetivo de regulamentar seu uso, promovendo a racionalização e a preservação do Patrimônio Arquivístico Digital do Estado.

A SECRETARIA DE ESTADO DA ADMINISTRAÇÃO, órgão central e normativo do Sistema Administrativo de Gestão Documental e Publicação Oficial, considerando o art. 126, III,"d", da Lei Complementar nº 741, de 12 de junho de 2019, e nos termos da Lei nº 9.747, de 26 de novembro de 1994, do Decreto nº 1.444, de 23 de março de 1988, e do Decreto nº 902, de 21 de outubro de 2020 e, ainda, conforme processo SEA 11166/2025,

RESOLVE:

Art. 1º Estabelecer diretrizes para a produção, organização, gestão, comunicação e preservação de documentos digitais no âmbito do Sistema Administrativo de Gestão Documental e Publicação Oficial (SGDPO), garantindo a conformidade com as normas arquivísticas vigentes e com os princípios da transparência, autenticidade, integridade e acessibilidade da informação.

Art. 2º Para fins desta Instrução Normativa, consideram-se as seguintes definições:

I – Documento: unidade de registro de informações, independentemente do suporte ou formato.

II – Documento arquivístico: aquele produzido ou recebido no curso de uma atividade prática, dotado de organicidade, ou seja, relacionado às funções e atividades da instituição ou indivíduo que o gerou.

III – Documento eletrônico: registro de informações criado, armazenado e transmitido em meio digital, acessível por sistemas eletrônicos.

IV – Documento não-digital: aquele que foi originalmente produzido em suporte físico, como papel, filme, fita magnética, entre outros.

V – Documento digital: documento eletrônico representado por códigos binários, permitindo sua manipulação por softwares e garantindo autenticidade por meio de tecnologias como certificação digital.

VI – Documento nato-digital: documento gerado diretamente em ambiente digital, sem versão física anterior, garantindo sua autenticidade por sistemas eletrônicos.

VII – Documento digitalizado: representação digital de um documento originalmente físico, obtido por meio de processos como a digitalização via scanner ou equipamento similar.

VIII – Comunicação eletrônica: toda troca de informações realizada por meios digitais, incluindo, mas não se limitando a, e-mails institucionais, mensagens instantâneas, videoconferências, sistemas eletrônicos e demais plataformas digitais utilizadas para a comunicação interna e externa dos órgãos e entidades da Administração Pública Estadual.

IX – Formato: estrutura física ou digital de um documento, determinando como suas informações são organizadas e armazenadas.

X – Informação: conjunto de dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

XI – Dado: é um elemento bruto, sem contexto ou interpretação.

XII – Autenticação: processo que assegura a integridade e a origem de um documento digital, por meio de mecanismos como assinaturas digitais e certificados eletrônicos.

XIII – Validade jurídica: a validade jurídica dos documentos digitalizados é garantida mediante atendimento aos requisitos técnicos e procedimentais previstos na legislação vigente, assegurando integridade, autenticidade, rastreabilidade e auditabilidade, conforme disposto no Decreto Federal 10.278/2020.

XIV – Assinatura eletrônica: qualquer método digital utilizado para demonstrar a concordância de uma pessoa com um documento eletrônico. Pode ser classificada em três níveis:

a. Assinatura eletrônica simples: aquela que permite identificar o signatário e associar os dados eletrônicos a ele, sendo admitida em transações de baixo risco e em documentos que não contenham informações protegidas por grau elevado de sigilo ou sensibilidade.

b. Assinatura eletrônica avançada: aquela que utiliza mecanismos de autenticação que asseguram a autoria e a integridade do documento eletrônico, como autenticação em dois fatores, biometria, chaves criptográficas ou outras tecnologias que ofereçam grau equivalente de segurança.

c. Assinatura eletrônica qualificada: aquela realizada com o uso de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, possuindo presunção de veracidade quanto à autoria e integridade dos documentos assinados, nos termos da legislação vigente.

XV – Assinatura digital: tipo específico de assinatura eletrônica baseada em criptografia assimétrica e certificados digitais emitidos por Autoridades Certificadoras (ACs). Garante a identidade do signatário, a integridade do documento e a característica de não repúdio, impedindo que o signatário negue sua autoria posteriormente.

XVI – Gestão de documentos: o conjunto de procedimentos e operações técnicas referentes à produção, classificação, tramitação, uso, acesso, avaliação, preservação e arquivamento dos documentos, pela temporalidade necessária, independentemente do formato ou suporte, visando a sua eliminação ou recolhimento para guarda permanente.

XVII – Repositório Arquivístico Digital Confiável (RDC-Arq): repositório digital que é capaz de manter íntegros os documentos digitais, de preservá-los e de garantir acesso aos mesmos pelo tempo necessário.

Art. 3º Os órgãos setoriais e seccionais do SGDPO deverão analisar e identificar, entre os documentos digitais sob sua responsabilidade, aqueles que possuem valor arquivístico, considerando sua relação com as funções institucionais, competências legais e atividades desempenhadas. Esse processo deve assegurar a correta classificação, gestão e preservação dos documentos, em conformidade com as diretrizes arquivísticas vigentes.

Art. 4º Os documentos digitais gerados ou recebidos no exercício das funções institucionais, como e-mails institucionais, mensagens instantâneas, gravações de reuniões, peças publicitárias, publicações em redes sociais, vídeos institucionais, materiais relacionados a cursos online, e outros equivalentes, devem ser avaliados quanto ao seu valor arquivístico, constar do PCD e TTD, ser classificados e armazenados conforme as normas vigentes estabelecidas pelo Órgão Central do SGDPO.

§ 1º Os documentos digitais devem ser identificados, classificados e armazenados, preferencialmente, em sistemas de gestão arquivística de documentos digitais, garantindo autenticidade, integridade, acessibilidade e preservação da informação, conforme o PCD e a TTD das atividades-meio e atividades-fim, conforme o caso.

§ 2º A captura, o registro e o arquivamento dos documentos digitais deverão garantir sua autenticidade e acessibilidade, utilizando formatos abertos e preserváveis, como PDF/A, XML ou equivalentes, conforme diretrizes de preservação digital.

§ 3º As publicações realizadas em redes sociais oficiais dos órgãos e entidades da Administração Pública Estadual devem ser capturadas e arquivadas periodicamente, garantindo sua preservação conforme as diretrizes de gestão documental estabelecidas

pelo Órgão Central do SGDPO.

§ 4º A captura, a exportação e o arquivamento devem considerar a preservação do conteúdo publicado, metadados, interações relevantes e contexto institucional, utilizando-se tecnologias compatíveis com a longevidade e autenticidade dos registros digitais.

§ 5º Na impossibilidade de arquivar diretamente as publicações em redes sociais, o registro poderá ser substituído pela guarda do plano de comunicação correspondente, que deverá conter o planejamento estratégico, o conteúdo publicado, a data de veiculação e demais informações relevantes para documentar a ação institucional.

§ 6º Os órgãos e entidades devem definir fluxos e metodologias para a preservação de publicações digitais, observando normas arquivísticas e de transparência, garantindo a rastreabilidade das ações institucionais.

§ 7º O monitoramento das redes sociais deve assegurar que os conteúdos sejam mantidos para preservação e respeitem os princípios de autenticidade, integridade e acessibilidade, além de conformidade com as normativas vigentes de proteção de dados e comunicação pública.

§ 8º Na ausência de um sistema de gestão arquivística de documentos digitais, os documentos deverão ser administrados pelos sistemas de negócio responsáveis por sua geração ou armazenamento, assegurando autenticidade, integridade, acessibilidade e rastreabilidade, em conformidade com as normas arquivísticas e de preservação digital vigentes.

Art. 5º A gestão dos documentos arquivísticos digitais deverá assegurar os seguintes atributos, conforme as diretrizes do e-ARQ Brasil e das normas arquivísticas vigentes:

I – Autenticidade: garantia da autoria, origem e data de produção, sem alterações indevidas;

II – Confiabilidade: capacidade de refletir fielmente os fatos, decisões ou atividades documentadas;

III – Fidelidade: correspondência exata com o conteúdo e contexto da transação original;

IV – Acessibilidade: possibilidade de recuperação e utilização por usuários autorizados, independentemente da tecnologia;

V – Identificação do contexto: clareza quanto ao processo de produção, remetente, destinatário, data e função documental, possibilitando a reconstituição do contexto de produção;

VI – Organicidade: relação orgânica com outros documentos produzidos no contexto institucional, refletindo as atividades e funções da entidade.

Art. 6º Os documentos digitais produzidos ou recebidos no âmbito da administração pública devem ser classificados conforme os planos de classificação de documentos e submetidos às tabelas de temporalidade, em conformidade com as normas vigentes no âmbito do SGDPO.

§1º A classificação dos documentos digitais deve considerar sua função administrativa, valor histórico e relevância jurídica, garantindo sua correta organização e destinação.

§2º O prazo de guarda, eliminação ou preservação permanente dos documentos digitais obedece às mesmas diretrizes estabelecidas para os documentos físicos, assegurando gestão documental eficiente e conformidade legal.

§3º Os procedimentos de avaliação e destinação dos documentos digitais devem estar alinhados com a legislação arquivística vigente, garantindo sua autenticidade, integridade e acessibilidade ao longo do tempo.

§4º A eliminação de documentos digitais deve ser precedida de autorização formal, seguindo critérios de segurança e rastreabilidade que garantam a irreversibilidade do processo.

§5º As ferramentas tecnológicas utilizadas na gestão de documentos públicos em suporte digital devem prever mecanismos que garantam a gestão, classificação e destinação documental, assegurando conformidade com as normativas específicas do órgão central do SGDPO.

Art. 7º Cabe à Diretoria do Arquivo Público, núcleo técnico do SGDPO, normatizar, supervisionar e orientar os agentes públicos quanto à aplicação de ferramentas tecnológicas na produção, gestão e preservação de documentos digitais.

Art. 8º Os órgãos e entidades da Administração Pública Estadual deverão adotar padrões abertos, interoperáveis e compatíveis com os princípios da preservação digital, assegurando a compatibilidade entre sistemas para a produção, armazenamento e compartilhamento de documentos digitais, garantindo sua integridade, longevidade e acesso contínuo, com o objetivo de preservar o patrimônio documental digital do Estado.

Art. 9º A segurança da informação deve ser garantida em todas as fases do ciclo de vida dos documentos digitais, adotando-se medidas de proteção contra acessos não autorizados, perda, alteração ou destruição dos documentos.

Parágrafo único. Compete aos órgãos setoriais e seccionais do SGDPO implementar políticas de segurança da informação, sob coordenação do órgão central do Sistema Administrativo de Ciência, Tecnologia e Inovação.

Art. 10 Os órgãos e entidades da Administração Pública Estadual devem promover a capacitação contínua dos agentes públicos em gestão documental e tecnologias da informação, com foco na produção, organização, preservação e acesso a documentos digitais, assegurando o correto manuseio, guarda e conformidade com as normas arquivísticas vigentes.

Art. 11 As ferramentas tecnológicas e sistemas informatizados utilizados na gestão de documentos digitais devem estar em conformidade com as normas e padrões técnicos estabelecidos pelo núcleo técnico do SGDPO.

Art. 12 Compete ao núcleo técnico do SGDPO acompanhar e realizar auditorias periódicas nos sistemas de gestão documental dos órgãos e entidades, com o objetivo de verificar a conformidade com esta Instrução Normativa e as boas práticas de gestão documental e preservação digital.

Art. 13 Cabe aos órgãos e entidades integrantes do SGDPO estabelecer fluxos de trabalho claros e definir as responsabilidades para a gestão dos documentos avulsos, garantindo sua rastreabilidade ao longo de seu ciclo de vida e assegurando a conformidade com as normas arquivísticas vigentes.

Art. 14 Os órgãos devem manter um controle eficaz de acesso aos usuários dos sistemas informatizados utilizados para a criação e gerenciamento desses documentos, garantindo monitoramento contínuo e atualizações regulares nos sistemas para assegurar a integridade, a segurança e a preservação da informação.

Art. 15 As assinaturas eletrônicas utilizadas nos órgãos e entidades do Estado de Santa Catarina serão classificadas nas seguintes modalidades:

I – Assinatura eletrônica simples: utilizada para documentos de menor impacto administrativo, que não envolvam sigilo ou sensibilidade jurídica;

II – Assinatura eletrônica avançada: utilizada para atos administrativos que requeiram maior segurança e identidade do assinante, conforme padrões estabelecidos pela autoridade certificadora do Estado;

III – Assinatura eletrônica qualificada (ICP-Brasil): obrigatória para documentos que exijam fé pública, contratos, atos normativos, convênios e outros instrumentos administrativos de alto impacto.

Parágrafo único. A adoção de assinaturas eletrônicas visa garantir a autenticidade, integridade, validade jurídica e confiabilidade dos documentos digitais, reduzindo custos operacionais e promovendo maior eficiência na tramitação de processos administrativos.

Art. 16 As assinaturas digitais realizadas em documentos públicos por meio de certificados emitidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) são

juridicamente válidas e possuem efeito legal, desde que o certificado utilizado estivesse vigente e ativo no momento da assinatura.

§1º A expiração do certificado digital não invalida as assinaturas feitas anteriormente em documentos públicos, pois a verificação da autenticidade e da integridade do documento é baseada no período em que o certificado estava válido.

§2º Após a expiração do certificado digital, este não poderá mais ser utilizado para novas assinaturas em documentos públicos, sendo necessário solicitar sua renovação ou a emissão de um novo certificado junto a uma Autoridade Certificadora credenciada.

I – Os documentos públicos assinados eletronicamente devem utilizar métodos de assinatura que garantam autenticidade, integridade e não repúdio, conforme previsto na legislação vigente.

Art. 17 A validação da assinatura eletrônica deve ser realizada por meio de ferramentas apropriadas, verificando a autenticidade do signatário, a integridade do documento e a conformidade com os requisitos legais.

§1º O processo de validação pode incluir a conferência da cadeia de certificação, quando aplicável, a verificação da validade temporal da assinatura e a identificação do método de autenticação utilizado.

§2º As assinaturas digitais qualificadas devem ser verificadas por sistemas de certificação oficiais, enquanto assinaturas avançadas e simples podem requerer mecanismos de confirmação adicionais, como autenticação em duas etapas, biometria ou registros de auditoria para garantir a autenticidade e não repúdio.

Art. 18 A exigência ou escolha do tipo de assinatura eletrônica deve ser compatível com a natureza e o grau de sensibilidade do documento público a ser firmado, devendo-se considerar:

I – Assinatura Eletrônica Simples: aplicável a documentos que não exigem alto nível de segurança, vincula o signatário ao documento por meio de dados básicos, como login e senha.

II – Assinatura Eletrônica Avançada: utilizada em documentos que requerem maior segurança, empregando autenticação biométrica ou múltiplas etapas de verificação.

III – Assinatura Eletrônica Qualificada: realizada com certificado digital emitido por Autoridade Certificadora credenciada na ICP-Brasil, garantindo máxima validade jurídica.

Art. 19 Os documentos públicos assinados eletronicamente devem ser armazenados de forma que preservem sua integridade, autenticidade e acessibilidade por prazo compatível com sua finalidade administrativa e legal.

§1º O armazenamento deve ocorrer em sistemas que permitam a recuperação do documento assinado, assegurando mecanismos de auditoria e rastreabilidade.

§2º Os documentos assinados digitalmente devem ser vinculados a métodos de preservação digital que garantam sua longevidade, impedindo alterações não autorizadas.

Art. 20 Em casos de comprometimento do certificado digital, erro ou indícios de fraude, a revogação da assinatura eletrônica pode ser solicitada por meio dos canais oficiais das Autoridades Certificadoras ou órgãos competentes.

§1º Os documentos públicos assinados eletronicamente devem estar sujeitos a auditorias periódicas para verificar conformidade com as normas de integridade e autenticidade.

§ 2º As contestações ou revogações de assinaturas eletrônicas devem ser realizadas conforme os procedimentos previstos nos regulamentos do órgão responsável pela administração do sistema assinador, assegurando a rastreabilidade, autenticidade e conformidade com as normas vigentes.

Art. 21 Os órgãos setoriais e seccionais do SGDPO que pretendam contratar ou implementar ferramentas tecnológicas para a gestão de informações e documentos públicos devem submeter previamente suas propostas ao órgão central do Sistema Administrativo para análise e validação.

§1º A avaliação do órgão central abrangerá, entre outros aspectos:

I – Adequação aos requisitos de classificação e temporalidade documental estabelecidos pelas normativas vigentes;

II – Capacidade de preservação, autenticidade e acessibilidade dos documentos digitais ao longo do tempo;

III – Compatibilidade com normas e padrões de interoperabilidade adotados pela administração pública;

IV – Segurança e rastreabilidade das informações registradas na ferramenta tecnológica;

V – Conformidade com diretrizes arquivísticas e legais aplicáveis à gestão documental.

§2º Somente após a validação do órgão central poderá ser formalizada a contratação ou a implantação da ferramenta tecnológica, assegurando a uniformidade, eficiência e segurança na gestão documental pública.

§3º Na especificação tecnológica da contratação, devem ser definidos os

requisitos mínimos de projeto e implementação, de acordo com as diretrizes estabelecidas no processo de gestão documental, assegurando conformidade, eficiência e segurança na administração dos documentos públicos, conforme diretrizes estabelecidas pelo órgão central do SGDPO.

Art. 22 – Os documentos emitidos por órgãos públicos, cuja autenticidade possa ser verificada por meio de código de validação digital, serão considerados autênticos para todos os efeitos legais.

§1º A validação da autenticidade do documento deverá ser realizada pelo agente público responsável, quando este não for o emissor do documento.

§2º Caso o documento tenha sido recebido como cópia, sua validação deverá indicar se trata-se de cópia autenticada administrativamente ou cópia simples, conforme as normativas vigentes.

§3º O sistema de tramitação desses documentos deverá garantir sua integridade, rastreabilidade e confiabilidade, em conformidade com o Decreto Federal nº 10.278/2020 e demais normativas aplicáveis.

Art. 23 A gestão de documentos públicos digitais deve garantir o equilíbrio entre transparência e proteção de dados pessoais, observando os dispositivos da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD).

§1º O acesso aos documentos digitais será regulado conforme seu grau de sigilo, observando-se as seguintes classificações:

I – Público: documento acessível a qualquer cidadão, conforme princípio da transparência.

II – Restrito: documento de acesso condicionado, limitado a agentes públicos autorizados ou a partes interessadas.

III – Sigiloso: documento protegido por restrições legais, cujo acesso depende de justificativa específica e cumprimento de requisitos normativos.

§2º Os órgãos públicos deverão implementar controles de acesso, garantindo que somente usuários autorizados possam visualizar, editar ou excluir documentos sensíveis, assegurando mecanismos de autenticação e rastreabilidade.

§3º No tratamento de dados pessoais em documentos digitais, devem ser aplicadas as diretrizes da LGPD, garantindo:

I – Finalidade específica e legítima para coleta e armazenamento dos dados.

II – Adoção de medidas técnicas e administrativas para a proteção contra acessos não autorizados.

III – Garantia de direitos dos titulares dos dados, incluindo acesso, retificação e eliminação conforme legislação.

§4º A divulgação de documentos públicos digitais que contenham dados pessoais deve ser precedida de análise sobre a necessidade de anonimizá-los ou restringir seu acesso, conforme previsto na LGPD e na LAI.

§5º Os sistemas utilizados na gestão de documentos digitais devem prever mecanismos de segurança digital, incluindo autenticação de usuários, controle de permissões, registro de acessos e proteção contra violações.

Art. 24 Esta Instrução Normativa entrará em vigor na data de sua publicação, ficando revogada a Instrução Normativa SEA nº 10/2006.

VANIO BOING
Secretário de Estado da Administração

RODRIGO FERNANDO BEIRÃO
Diretor do Arquivo Público