Conarq

DIRETRIZES PARA A PRESUNÇÃO DE AUTENTICIDADE DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Conarq
CONSELHO NACIONAL DE ARQUIVOS

Câmara Técnica de Documentos Eletrônicos

MINISTÉRIO DA JUSTIÇA
ARQUIVO NACIONAL
CONSELHO NACIONAL DE ARQUIVOS

RESOLUÇÃO Nº 37, DE 19 DE DEZEMBRO DE 2012

Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais

Anexo

Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais

MINISTÉRIO DA JUSTIÇA
ARQUIVO NACIONAL
CONSELHO NACIONAL DE ARQUIVOS

RESOLUÇÃO Nº 37, DE 19 DE DEZEMBRO DE 2012

Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais

O PRESIDENTE DO CONSELHO NACIONAL DE ARQUIVOS - CONARQ, no uso de suas atribuições, previstas no item IX do art. 23 de seu Regimento Interno, aprovado pela Portaria nº. 2.588, do Ministério da Justiça, de 24 de novembro de 2011, em conformidade com a deliberação do Plenário em sua 68ª reunião plenária do CONARQ, realizada no dia 5 de dezembro de 2012,

Considerando que é dever do Poder Público a gestão documental, a proteção especial aos documentos de arquivo e as providências para franquear aos cidadãos as informações contidas na documentação governamental;

Considerando que o Conselho Nacional de Arquivos tem por finalidade definir a política nacional de arquivos públicos e privados e exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo, independentemente da forma ou do suporte em que a informação está registrada;

Considerando que a organização dos arquivos e o gerenciamento das informações neles contidas se constituem em instrumento de eficácia administrativa, contribuindo para a modernização da administração pública;

Considerando que as organizações públicas e privadas e os cidadãos vêm cada vez mais produzindo documentos arquivísticos digitais e que governos, organizações e cidadãos dependem do documento digital como fonte de prova e de informação, e para garantia de direitos;

Considerando que os documentos arquivísticos digitais podem se apresentar na forma de texto, imagem fixa ou em movimento, áudio, base de dados, planilha e outras num repertório crescente de possibilidades;

Considerando que os documentos digitais são suscetíveis à alteração, lícita ou ilícita, à degradação física e à obsolescência tecnológica de hardware, software e formatos, as quais podem colocar em risco sua autenticidade;

Considerando que a gestão arquivística de documentos, independentemente da forma ou do suporte adotados, tem por objetivo garantir a produção, a manutenção e a preservação de documentos arquivísticos confiáveis e autênticos;

Considerando o conceito de autenticidade dos documentos a partir da Arquivologia e da Diplomática;

Considerando a Resolução nº 24, de 3 de agosto de 2006, que estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas.

RESOLVE:

Art. 1º Aprovar as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais, disponibilizadas no sitio do CONARQ, em: http://www.conarq.arquivonacional.gov.br.

§ 1º As Diretrizes de que trata essa resolução têm por finalidade instrumentalizar os produtores e custodiadores de documentos arquivísticos para essa presunção da autenticidade desses documentos.

§ 2º A autenticidade dos documentos arquivísticos digitais deve estar apoiada em procedimentos de gestão arquivística de documentos.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

JAIME ANTUNES DA SILVA

[Publicado no Diário Oficial da União, Edição nº 245, de 20 de dezembro de 2012 - Seção 1]

Câmara Técnica de Documentos Eletrônicos

Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais

dezembro 2012

I – Introdução

A autenticidade dos documentos arquivísticos digitais é ameaçada sempre que eles são transmitidos através do espaço (entre pessoas e sistemas ou aplicativos) ou do tempo (armazenagem contínua ou atualização/substituição de *hardware*/*software* usados para armazenar, processar e comunicar os documentos). Como a guarda de documentos arquivísticos digitais é inexoravelmente ameaçada pela obsolescência tecnológica, a presunção da sua autenticidade deve se apoiar na evidência de que eles foram mantidos com uso de tecnologias e procedimentos administrativos que garantiram a sua identidade e integridade (componentes da autenticidade); ou que, pelo menos, minimizaram os riscos de modificações dos documentos a partir do momento em que foram salvos pela primeira vez e em todos os acessos subsequentes.

A presunção de autenticidade dos documentos arquivísticos sempre fez parte do processo tradicional de avaliação desses documentos e é fortemente apoiada na análise de sua forma e de seu conteúdo, que nos documentos não digitais estão inextricavelmente ligados ao suporte – isto é, forma, conteúdo e suporte são inseparáveis. Além disso, essa presunção baseia-se na confirmação da existência de uma cadeia de custódia ininterrupta,[1] desde o momento da produção do documento até a sua transferência para a instituição arquivística responsável pela sua preservação no longo prazo. Caso essa cadeia de custódia seja interrompida, o tempo em que os documentos não estiveram sob a proteção do seu produtor ou sucessor pode causar muitas dúvidas sobre a sua autenticidade.

Os documentos arquivísticos digitais apresentam dificuldades adicionais para presunção de autenticidade em razão de serem facilmente duplicados, distribuídos, renomeados, reformatados ou convertidos, além de poderem ser alterados e falsificados com facilidade, sem deixar rastros aparentes. Assim, a presunção de autenticidade do documento arquivístico digital é realizada por meio da análise da sua forma e do seu conteúdo, bem como do ambiente de produção, manutenção/uso e preservação desse documento, e não apenas com base em suas características físicas ou em soluções tecnológicas.

As características físicas de documentos digitais, isto é, suporte e cadeias de *bits* neles registradas, podem mudar ao longo do tempo. A mudança de suporte não compromete a autenticidade do documento digital porque, nesse caso, diferentemente dos documentos não digitais, forma e conteúdo estão desvinculados do suporte. Com relação às cadeias de *bits*, em primeiro lugar é preciso esclarecer que, quando um documento digital é salvo, ele é desmontado em uma ou mais cadeias de *bits* que contêm os dados de forma,

1 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.

conteúdo e composição. Algumas estratégias de preservação digital, baseadas na conversão de formatos, implicam alteração das cadeias de *bits*. Essa alteração deve manter a forma do documento originalmente produzido, e com isso apoiar a autenticidade do documento digital.

É importante esclarecer que o documento arquivístico digital é o objeto conceitual, isto é, aquele normalmente apresentado em dispositivo de saída (monitor, caixa de som), e não o objeto físico (as cadeias de *bits* registradas em um suporte). As cadeias de *bits* são necessárias para que o documento arquivístico seja apresentado, mas não se constituem nesse documento.

II – Conceitos

As diretrizes aqui apontadas estão baseadas nos seguintes conceitos:

1. Autenticidade: qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração. A autenticidade é composta de identidade e integridade.

    - Identidade é o conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos (ex.: data, autor, destinatário, assunto, número identificador, número de protocolo).

    - Integridade é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção (sem sofrer alterações de forma e conteúdo) de maneira a atingir seus objetivos.

    - Identidade e integridade são constatadas à luz do contexto (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico) no qual o documento arquivístico foi produzido e usado ao longo do tempo.

2. Autenticação: declaração de autenticidade de um documento arquivístico, num determinado momento, resultante do acréscimo de um elemento ou da afirmação por parte de uma pessoa investida de autoridade para tal.

3. Documento autêntico: documento que teve sua identidade e integridade mantidas ao longo do tempo.

4. Documento arquivístico: documento produzido ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e retido para ação ou referência.

5. Documento digital: informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional.

6. Documento arquivístico digital: documento digital reconhecido e tratado como um documento arquivístico.

7. Forma: aparência ou apresentação do documento.

8. Conteúdo: informação contida no documento.

9. Composição: relação entre os dados de forma e conteúdo do documento digital que permite sua apresentação.

10. Presunção de autenticidade: inferência da autenticidade de um documento arquivístico feita a partir de fatos conhecidos sobre a maneira como aquele documento foi produzido e mantido.

11. Confiabilidade: credibilidade de um documento arquivístico enquanto 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.

III – Da autenticidade de documentos arquivísticos

A autenticidade de documentos arquivísticos envolve três aspectos importantes: legal, diplomático[2] e histórico.

Documentos legalmente autênticos são aqueles que dão testemunhos sobre si mesmos em virtude da intervenção, durante ou após sua produção, de uma autoridade pública representativa, garantindo sua genuinidade.

Documentos diplomaticamente autênticos são aqueles que foram escritos de acordo com a prática do tempo e do lugar indicados no texto e assinados pela pessoa (ou pessoas) competente para produzi-los.

Documentos historicamente autênticos são aqueles que atestam eventos que de fato aconteceram ou informações verdadeiras.

Os três aspectos da autenticidade acima referidos são independentes um do outro, de tal maneira que um documento não atestado por uma autoridade pode ser diplomática e historicamente autêntico, mas sempre será legalmente inautêntico. Um breve papal que não contenha a expressão *datum... sub anulo piscatores* pode ser legal e historicamente autêntico, mas é inautêntico do ponto de vista diplomático. Um certificado emitido por uma

2 Referente à diplomática, disciplina que tem como objeto o estudo da estrutura formal e da confiabilidade e autenticidade dos documentos.

autoridade pública segundo as regras burocráticas, mas contendo informação que não corresponde à realidade, é legal e diplomaticamente autêntico, mas historicamente falso.

Observa-se uma relação entre o aspecto histórico da autenticidade e o conceito diplomático de confiabilidade no sentido de que ambos se referem à veracidade do conteúdo do *documento.* Já no que tange ao ponto de vista da diplomática, a autenticidade se refere a não alteração do documento após sua produção, mesmo que o conteúdo não seja verdadeiro. Para fins destas diretrizes será considerado o conceito de autenticidade da diplomática.

IV – Presunção de autenticidade dos documentos arquivísticos digitais

Conforme mencionado anteriormente, a presunção de autenticidade do documento arquivístico digital se dá com base na análise da forma e do conteúdo e no ambiente de produção, manutenção/uso e preservação desse documento. Esse ambiente compreende: procedimentos de controle, o sistema informatizado e o próprio produtor e/ou custodiador dos documentos.

Os procedimentos de controle compreendem quem produz, mantém/usa e preserva os documentos arquivísticos digitais e como essas ações são realizadas. Assim, é preciso que se definam direitos de acesso, espaços de trabalho (produção, recebimento, alteração, classificação, registro de metadados, arquivamento e destinação), conjunto de metadados e procedimentos de preservação.

O sistema informatizado tem que ser confiável. Para tanto deve incluir trilhas de auditoria, controle de acesso de usuários, métodos robustos para garantir a integridade dos documentos (como *checksum*[3] ou *hash*[4]), meios de armazenamento estáveis e medidas de segurança para controlar o acesso indevido à infraestrutura tecnológica (computadores, redes e dispositivos de armazenamento).

A entidade produtora e/ou custodiadora dos documentos arquivísticos digitais tem de possuir reputação idônea, demonstrar capacidade e conhecimento específico para gerenciar os documentos e, consequentemente, inspirar a confiança dos usuários.

---

3 Valor, calculado a partir dos dados, que permite verificar se houve alteração.

4 É o resultado da ação de algoritmos que fazem o mapeamento de uma sequência de *bits* de tamanho arbitrário para uma sequência de *bits* de tamanho fixo menor, conhecido como resultado *hash*, de forma que seja muito difícil encontrar dois documentos digitais produzindo o mesmo resultado *hash* e que o processo reverso também não seja realizável (a partir de um *hash*, não é possível recompor o documento digital que o gerou).

A adoção dos requisitos acima implica o estabelecimento e a aplicação contínua e efetiva de políticas e procedimentos administrativos, fornecendo, dessa forma, a melhor evidência para apoiar a presunção de autenticidade dos documentos arquivísticos digitais, independentemente de mecanismos tecnológicos de autenticação.

Nesse sentido, devem-se implementar, sempre que possível, técnicas de autenticação apoiadas em políticas e procedimentos administrativos e arquivísticos independentes de tecnologia e/ou neutros.

V – Autenticação dependente de tecnologia

Técnicas de autenticação dependentes de tecnologia, tal como a assinatura digital, são usadas para fornecer um mecanismo tecnológico que declara a autenticidade dos documentos digitais em um dado momento.

É preciso esclarecer que autenticação é diferente de autenticidade. A autenticidade é a qualidade de o documento ser verdadeiro, isto é, ser exatamente aquele que foi produzido, ao passo que autenticação é a declaração da autenticidade feita em um dado momento por uma pessoa autorizada para tal. Enquanto declaração, a autenticação não garante necessariamente a autenticidade do documento, na medida em que se pode declarar como autêntico algo que não é. Da mesma forma, um documento pode ser considerado autêntico sem que nele conste uma autenticação.

Uma boa utilização da assinatura digital se dá quando os documentos digitais são transmitidos no espaço, ou seja, entre pessoas, sistemas ou aplicativos, de forma a permitir um ambiente de confiabilidade nas transações. No Brasil, o valor legal da assinatura digital foi reconhecido.[5] No entanto, as técnicas de autenticação baseadas em tecnologia não são efetivas para a transmissão dos documentos no tempo, ou seja, quando são armazenados no longo prazo ou quando há atualização/substituição de *hardware*, *software* ou formatos. Isto porque, em virtude do seu objetivo e de sua forma de funcionamento, as assinaturas digitais não podem ser migradas para as novas cadeias de *bits* resultantes da conversão dos documentos para outros formatos de arquivo.

A assinatura digital é resultado de um cálculo matemático que envolve a cadeia de *bits* do documento e a chave da assinatura digital. Se a cadeia de *bits* for alterada, por motivo de corrompimento, adulteração ou conversão, a assinatura não corresponderá mais a essa nova cadeia de *bits* e não poderá mais garantir a autenticidade do documento. Isto porque, embora o documento conceitual seja o mesmo, passará a estar relacionado a uma nova

5 Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

cadeia de *bits*, que não tem mais a assinatura. Desta forma, a assinatura digital garante somente a integridade da cadeia de *bits* original, mas não a do documento conceitual ao longo do tempo.

Em razão da necessidade de conversões, a assinatura digital não garante a autenticidade do documento, no longo prazo, tornando-se necessários outros procedimentos de gestão e de preservação, como a inserção de metadados. Ao se receber um documento assinado digitalmente, deve-se registrar, como metadado de integridade, a informação indicando que o documento foi recebido com tal assinatura e que esta foi verificada. Da mesma maneira, nas sucessivas conversões de formatos, deve-se registrar, também como metadado, o evento de conversão.

Assim, a não ser que o desenvolvimento da tecnologia da assinatura digital permita que, ao longo do tempo, sua codificação seja preservada na nova cadeia de *bits* resultante das inevitáveis conversões, a autenticidade não é garantida por meio de assinatura digital.