SEÇÃO 10

INTEGRIDADE, AUTENTICIDADE E PROVA

IBERARCHIVOS IBERARQUIVOS
ARCHIVO NACIONAL COSTA RICA
UNIVERSIDAD DE COSTA RICA

MÓDULO 7

Gestão e preservação de documentos digitais

SEÇÃO 10

Integridade, autenticidade e prova

Adaptação do Arquivo Nacional da Costa Rica
Versão 1, 2024

Este curso foi traduzido e adaptado pela Direção Geral do Arquivo Nacional da Costa Rica, em colaboração com a Seção de Arquivologia da Universidade da Costa Rica, a partir do material original de 2011 da Associação Internacional de Arquivos Francófonos, disponível online no Portal Internacional Arquivístico Francófono. Esclarece-se que podem existir variações em relação ao conteúdo original. Para acessar o material em francês, visite https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques.

IBERARCHIVOS IBERARQUIVOS ARCHIVO NACIONAL COSTA RICA UNIVERSIDAD DE COSTA RICA

Conteúdo

Capítulo 1. Objetivo da seção

Nesta seção em uma primeira parte será apresentado o marco legal probatório que afetou todos os países no que diz respeito aos documentos eletrônicos, com base na experiência vivida na Costa Rica. Esse marco normativo tem como objetivo conferir o mesmo valor probatório aos documentos em formato digital que aos documentos em formato papel, em determinadas condições e devido ao contexto de uso crescente da Internet e das redes de comércio eletrônico. Além disso, serão apresentados os procedimentos de assinatura digital (criptografia de chave pública).

Um segundo tópico trata, nesse contexto, do desenvolvimento da administração eletrônica, como os programas de governo, aspectos gerais que estruturam esse desenvolvimento, questões específicas de interoperabilidade, o trabalho realizado pelo grupo InterPARES sobre a autenticidade em um ambiente digital, o arquivamento em planos de governo e as propostas para garantir a autenticidade dos documentos por meio do modelo OAIS.

Capítulo 2. O marco legal da prova na Costa Rica

Todos os países avançaram da mesma maneira com o estabelecimento de um novo marco legal que outorga, sob certas condições, o mesmo valor probatório aos documentos em formato digital que aos documentos em papel.

Na Costa Rica, o marco legal para esses efeitos está em vigor desde o ano de 2005 e é ilustrativo do desenvolvimento geral dos países. Por isso, sendo conhecedores dessa situação, optou-se por desenvolver aqui, como exemplo, esse marco costarriquenho, no qual se destaca o essencial.

Lei de Certificados, Assinaturas Digitais e Documentos Eletrônicos N.º 8454 de 30 de agosto de 2005

Até essa data, na Costa Rica, vigorava o princípio da inseparabilidade entre um suporte material duradouro e a informação nele contida, o que constituía a qualidade da prova e, em particular, da prova pré-constituída de um ato jurídico.

A Lei de Certificados, Assinaturas Digitais e Documentos Eletrônicos Nº 8454 de 30 de agosto de 2005 foi reformada em duas ocasiões, conforme indica o Sistema Costarriquenho de Informação Jurídica (SINALEVI, 2022) e desde a primeira versão da lei, estabelece-se a equivalência funcional entre a assinatura manuscrita e a assinatura digital certificada.

1. Portanto, confere-se a mesma força probatória aos documentos eletrônicos que aos documentos físicos, conforme se observa a seguir:

"Qualificação jurídica e força provatória. Os documentos eletrônicos serão qualificados como públicos ou privados, e lhes será reconhecida força probatória nas mesmas condições que aos documentos físicos." (Lei 8454,2005,art.4)**.**

Nesta lei, estabelece-se o âmbito de aplicação, o qual rege os setores público e privado na Costa Rica.
(Art.1).

Além disso, a lei estabelece uma série de exceções, conforme se observa a seguir

a) Os atos ou negócios nos quais, por determinação legal, a fixação física seja consubstancial.

b) As disposições por motivo de falecimento, com exceção do que é estabelecido nos artigos 183 da Lei 7732, Lei Reguladora do Mercado de Valores, de 17 de dezembro de 1997, e no artigo 95 da Lei 8956, Lei Reguladora do Contrato de Seguros, de 17 de junho de 2011.

Assim reformado o inciso anterior pelo artigo 1° da lei N° 10181 de 5 de maio de 2022)

c) Os atos e convenções relativos ao Direito de Família.

d) Os atos personalíssimos em geral.

(Nota do Sinalevi: Por meio do artigo 2, parágrafo X, da lei que aprova o Código Processual de Família, nº 9747, de 23 de outubro de 2019, este numeral será reformado. De acordo com o artigo transitório III da lei anteriormente mencionada, essa modificação entrará em vigor a partir de 1º de outubro de 2024, de modo que, a partir dessa data, o novo texto será o seguinte: "Artigo 5- Em particular e exceções Em particular, e sem que isso implique a exclusão de outros atos, contratos ou negócios jurídicos, a utilização de documentos eletrônicos é válida para o seguinte:

a) A formação, formalização e execução dos contratos.

b) A indicação para notificações conforme a Lei nº 7637, Lei de Notificações, Citações e outras Comunicações Judiciais, de 21 de outubro de 1996.
c) A tramitação, gestão e conservação de expedientes judiciais e administrativos; igualmente, o recebimento, prática e conservação de provas, incluindo as recebidas por arquivos e meios eletrônicos. Da mesma forma, os órgãos jurisdicionais que necessitarem da atualização de certificações e, em geral, de outras peças, poderão atuar com base em simples impressões dos documentos online feitas pela autoridade judicial ou aceitar as impressões desses documentos online, apresentadas pela parte interessada e certificadas notarialmente.

d) A emissão de certificações, atestados e outros documentos.

e) A apresentação, tramitação e inscrição de documentos no Registro Nacional.
f) A gestão, conservação e utilização, em geral, de protocolos notariais, incluindo a manifestação do consentimento e a assinatura das partes.

Não poderão ser consignados em documentos eletrônicos:

a) Os atos ou negócios nos quais, por determinação legal, a fixação física seja consubstancial.

b) As disposições por causa de morte.

c) Os atos e convenções não jurisdicionais relativos ao direito de família.

d) Os atos personalíssimos em geral.") (Art.5)

2. Na lei, estabelecem-se também diferentes conceitos relacionados à assinatura digital, tais como:

- Definição de assinatura digital:

  Alcance do conceito. Entende-se por assinatura digital qualquer conjunto de dados anexado ou logicamente associado a um documento eletrônico, que permita verificar sua integridade, bem como **identificar de forma inequívoca e vincular juridicamente o autor ao documento eletrônico.**

Uma assinatura digital será considerada certificada quando for emitida **com base em um certificado digital vigente, expedido por um certificador registrado.** (Art.8)

• Estabelece também o valor **equivalente**, pois explica claramente esse conceito conforme detalhado a seguir.

Valor equivalente. Os documentos e as comunicações assinados por meio de assinatura digital, terão **o mesmo valor e eficácia probatória de seus equivalentes assinados à mão.** Em qualquer norma jurídica que exija a presença de uma assinatura, serão igualmente reconhecidas tanto a digital quanto a manuscrita.

Os documentos públicos eletrônicos deverão conter a assinatura digital certificada.

(Art.9) • Determina a presunção de autoria e responsabilidade

Presunção de autoria e responsabilidade. Todo documento, mensagem eletrônica ou arquivo digital associado a uma assinatura digital certificada será presumido, salvo prova em contrário, como de autoria e responsabilidade do titular do correspondente certificado digital, vigente no momento de sua emissão.

Entretanto, **essa presunção não dispensa o cumprimento das formalidades adicionais de autenticação, certificação ou registro que, do ponto de vista jurídico, a lei exija para um ato ou negócio determinado.** (Art.10)

Ou seja, o documento assinado digitalmente deve cumprir todas as formalidades exigidas para o documento em papel.

2.1. A assinatura criptográfica com chave pública

Essa tecnologia tem sua origem no campo da criptografia, que pode ser definida como um processo de proteção da informação que consiste em encriptar, mascarar ou codificar os dados para que eles não possam ser acessados por pessoas não autorizadas.

Durante muitos anos, para poder comunicar informações cifradas entre si, as pessoas precisavam concordar com uma chave privada (secreta) para realizar o processo, como explicam Banat-Berger e Huc (2010), que mencionam que a informação cifrada se baseia em uma descoberta de dois pesquisadores da Universidade de Stanford, Whitfield Diffie e Martin Hellman, o mecanismo agora se baseia na separação da chave única em duas chaves distintas:

- uma chave privada
- e uma chave pública.

A chave privada é utilizada para a criptografia e a chave pública para a descriptografia. Esse mecanismo é conhecido como criptografia de chave pública ou criptografia assimétrica:

- com a chave privada utilizada para assinar
- e a chave pública utilizada para a verificação.

De fato, o mecanismo baseia-se em três elementos:

- a geração de uma impressão digital,
- assinar a impressão digital com uma chave privada (secreta)
- e estabelecer o vínculo entre a chave privada e seu proprietário.

2.1.1. Gerando uma "impressão digital"

A impressão digital, geralmente de tamanho fixo, é criada a partir do documento utilizando uma função matemática chamada função hash:

- esta função restaura uma impressão indissociável do documento do qual é extraída e que possui um comprimento fixo;
- a impressão digital é enviada junto com o documento
- ao chegar, com a mesma função, o sistema calcula uma impressão digital do documento recebido e compara as duas impressões digitais: se o resultado for o mesmo, isso significa que há uma probabilidade muito alta de que o documento não tenha sido manipulado durante a transmissão.

EXEMPLO
A menor modificação no arquivo resulta na geração de uma impressão digital completamente diferente

Considere o seguinte texto: "Algoritmo MD5 ("Wikipedia, a enciclopédia livre e aberta")"

A impressão digital de um arquivo de texto que contém apenas este texto, calculada com o algoritmo MD5, é a seguinte:
"d6aa97d33d459ea3670056e737c99a3d"

Modificando apenas um carácter deste texto: "MD5 ("Wikipedia, a enciclopédia livre e livre")" Esse selo se altera radicalmente e se transforma em: "5da8aa7126701c9840f99f8e9fa54976"

COMPLEMENTO: COMPROVAÇÃO DA INTEGRIDADE

É um elemento fundamental da preservação digital, que permite assegurar que o conteúdo digital não tenha sido perdido, modificado ou danificado.

Implica o uso de software para gerar uma soma de verificação que representa a estrutura do arquivo, de modo que, posteriormente, as somas de verificação geradas em diferentes momentos sejam conferidas para corroborar se houve alguma alteração.

Estas ferramentas são utilizadas para detectar se o conteúdo do arquivo ou sua assinatura digital mudou, mas não indica em que parte do arquivo foi produzida a mudança.

A verificação de integridade é utilizada para:

- Ao mover/transferir dados: ao receber conteúdo como depositante ou ao substituir os meios de armazenamento.
- Para comprovar o armazenamento: monitorar o arquivo digital ao longo do tempo.
- Para demonstrar a autenticidade: uma verificação da integridade documentada permite mostrar aos usuários a autenticidade do conteúdo digital.

A criação de várias cópias de cada objeto digital permite substituir qualquer arquivo danificado ou faltante caso seja detectado algum problema, manter essas cópias em diferentes locais e em diferentes tipos de meios de armazenamento ajuda a mitigar o risco de perda.

Existem ferramentas que permitem a comprovação da integridade:

DROID, FITS, FIXITY y CHECKSUM BY CORZ

2.1.2. Assinatura da impressão digital com a chave privada (secreta)

Durante a transmissão, o documento e sua assinatura digital poderiam ter sido roubados e substituídos por outro documento com sua própria impressão digital.

Esta é a razão

- a impressão digital inicial está assinada com a chave privada (secreta) de seu autor.
- e verifica-se a impressão digital gerada na chegada com a chave pública correspondente à chave privada, que é destinada a ser comunicada a todos aqueles que desejem verificar a assinatura.

Deste modo

- a assinatura também permite certificar a origem do documento: falamos então de “não repúdio” porque o autor não pode deixar de reconhecer ser o autor do ato, na medida em que a chave pública só pode verificar positivamente aquilo que foi assinado pela chave privada correspondente.

Representação sobre o mecanismo de assinatura. Fonte: Suporte da assinatura

2.1.3. Estabelecimento do vínculo entre a chave privada e seu titular

Finalmente, resta assegurar o vínculo entre a chave privada e seu proprietário. É aqui que entram os provedores de certificação com os quais você registrará sua chave pública. Assim, um terceiro (o provedor do serviço) garante que a chave pública é efetivamente do próprio titular e, dessa forma, cria um vínculo:

- insira a chave pública
- e sua identidade.

O registro é realizado em um certificado que contém uma certa quantidade de informações, que varia conforme o nível de segurança do certificado e do provedor de serviços:

- identidade de seu proprietário,
- qualidade,
- chave pública,
- entre outros.

Dois elementos muito importantes são

- por um lado, o período de validade do certificado (na Costa Rica é de quatro anos)
- por outro lado, as transações permitidas para este certificado.

Evidentemente, o certificado é assinado por sua vez com a chave privada do provedor de serviços. Isso implica que, assim que um sistema verifica uma chave pública, ele começa verificando a assinatura do certificado, antes de verificar a assinatura do documento enviado.

Pode-se acrescentar que o processo de assinatura digital, conforme descrito, tem como objetivo garantir a integridade do documento durante sua transferência e dar ao destinatário a certeza da identidade do remetente.

ATENÇÃO

Este processo não tem como objetivo garantir a confidencialidade do documento.

Essa confidencialidade só poderá ser obtida se o próprio documento estiver criptografado.

EXEMPLO

Criação de um certificado de assinatura digital, segundo sua hierarquia de emissão

Hierarquia de assinatura digital. Fonte: Suporte da assinatura

Este sistema relativamente complexo conduz à criação de uma infraestrutura de chave pública e percebe-se que a verificação de uma assinatura induz, junto com o documento propriamente dito, a conservação

• incluindo os algoritmos de assinatura utilizados no momento da assinatura do documento,

• assim como a dos certificados (é necessário basear-se naquele que era válido no momento em que o documento foi assinado).

Segue abaixo o Diagrama da hierarquia nacional de certificadores registrados na Costa Rica, conforme a Política de Certificados para a Hierarquia Nacional de Certificadores Registrados.

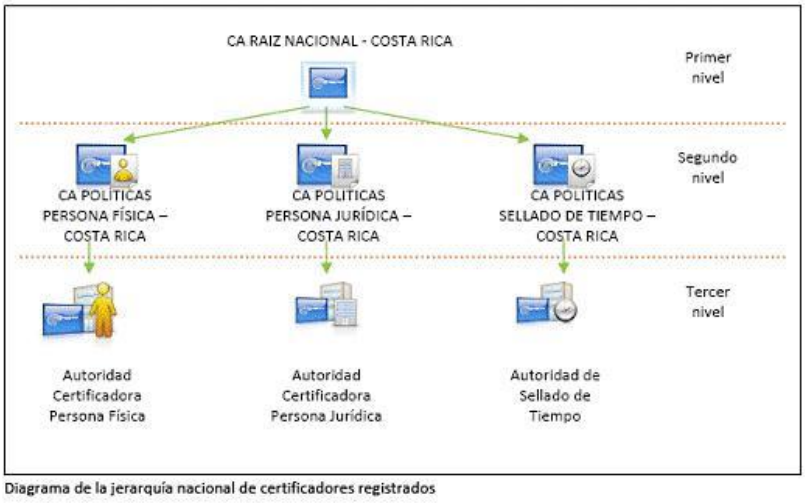


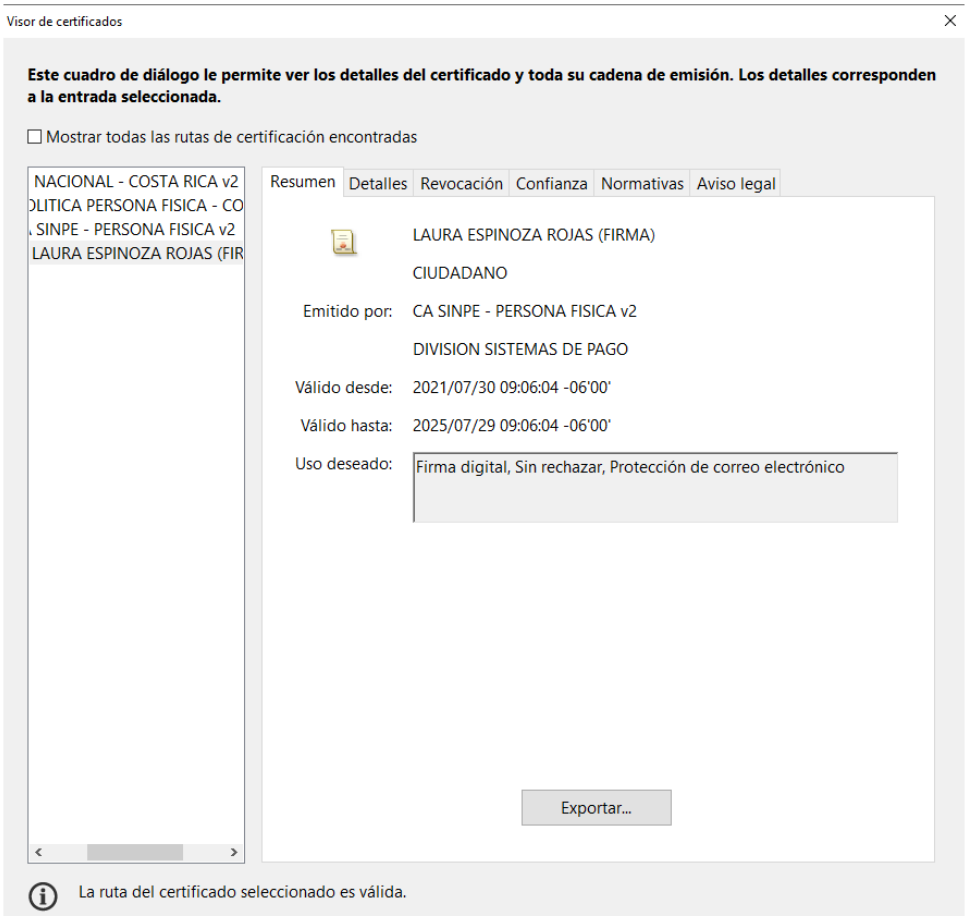
Diagrama de hierarquia nacional de certificadores registrados. Fonte: Suporte da assinatura

COMPLEMENTO: FUNCIONAMENTO DOS CERTIFICADOS

Cartão leitor de assinatura digital da Costa Rica. Fonte: Suporte da assinatura

Assim como é utilizado em criptografia e segurança da informação, um certificado eletrônico é um bloco de dados que contém, em um formato especificado, as seguintes partes:

- um número de série;
- a identificação do algoritmo de assinatura:
- a designação da autoridade certificadora emissora do certificado;
- o período de validade após o qual será suspenso ou revogado;
- o nome do titular da chave pública;
- a identificação do algoritmo de criptografia e o valor da chave pública constituída por um par de chaves assimétricas
- informação adicional opcional;
- a identificação do algoritmo de assinatura e o valor da assinatura digital



Interface de visibilidade dos certificados de assinatura digital

2.2. Regulamento da Lei de Certificados, Assinaturas Digitais e Documentos Eletrônicos Nº 33018

Este regulamento é emitido pelo Poder Executivo da Costa Rica (20 de março de 2006).

- serve para regulamentar e dar cumprimento à execução da Lei de Certificados, Assinaturas Digitais e Documentos Eletrônicos, número 8454
- respeita o caráter e a hierarquia de regulamento geral, nos termos do artigo 6 da Lei Geral da Administração Pública, em relação aos demais regulamentos particulares ou autônomos na matéria.

Ou seja, está abaixo das leis da República e acima dos regulamentos particulares ou autônomos que alguma instituição possa emitir sobre este tema.

O que diz este regulamento?

Contém um glossário sobre os termos que serão utilizados no âmbito nacional da assinatura digital certificada, determina que o conteúdo, as condições de emissão, suspensão, revogação e expiração dos certificados digitais serão aqueles indicados na Norma INTE/ISO 21188 em sua versão vigente e nas políticas que, para esse fim, emitir a Diretoria de Certificadores de Assinatura Digital.

Estabelece também as obrigações dos usuários dos certificados digitais, **o prazo de suspensão dos certificados, revogação por cessação das atividades de um certificador, reconhecimento jurídico** dos certificados digitais expedidos por certificadores registrados junto à Diretoria de Certificadores de Assinatura Digital, **comprovação de aptidão técnica e administrativa** para obter a condição de certificador registrado.

Fala também sobre **as formalidades do pedido** do certificador que desejar se registrar como tal, a **caução** que devem possuir os sujeitos privados que desejem prestar o serviço, entre outros aspectos. Além disso, estabelece as **funções**, atribuições e responsabilidades dos certificadores registrados.

Por outro lado, estabelece também as responsabilidades e funções da Diretoria de Certificadores de Assinatura Digital — pertencente ao Ministério de Ciência, Tecnologia e Telecomunicações — como órgão administrador e supervisor do Sistema Nacional de Certificação Digital. Essa Diretoria também deve contar com um **Comitê Assessor de Políticas** e, por fim, este regulamento menciona as diferentes sanções às quais um certificador pode estar sujeito.

2.3. Conclusões relativas a marco legal

O sistema legal vigente permite desmaterializar gradualmente os processos comerciais ao longo da cadeia. **Os conceitos de autenticação e integridade, compatíveis com os riscos da tecnologia digital quando se utilizam redes, são fundamentais, e são as tecnologias de criptografia de chave pública que são empregadas para cumprir esses requisitos.** São estabelecidas infraestruturas que permitem assegurar as trocas, as transações e o fluxo de dados intercambiados.

> Dessa forma, o Estado costarriquenho é o principal promotor da assinatura digital certificada com relevância jurídica, conforme a lei nº 8454, e pertence ao Ministério de Ciência, Inovação, Tecnologia e Telecomunicações (MICITT); além disso, é o órgão administrador e supervisor do **Sistema Nacional de Certificação Digital.** A entidade que quiser emitir

certificados digitais devem estar registrados junto à Diretoria de Certificadores de Assinatura Digital, e garantir o cumprimento das normas de segurança e operação mais rigorosas, **para que os documentos eletrônicos assinados digitalmente tenham o mesmo valor legal que os documentos físicos.**

Para registrar uma Autoridade Certificadora, deve-se garantir a competência legal e técnica, para esse fim, a Diretoria de Certificadores de Assinatura Digital conta com o apoio do Ente Costarriquenho de Acreditação (ECA), que é o responsável por avaliar o cumprimento dos requisitos técnicos e credenciar a Autoridade Certificadora.

Autoridades Certificadoras: A gestão para ser Autoridade Certificadora divide-se em duas fases: Na primeira fase, o solicitante implementa e garante a operação da infraestrutura de chave pública de acordo com a lei e seu regulamento. Na segunda fase, gerencia sua autorização ou registro diante da Direção Geral de Certificados e Assinaturas Digitais (DGDCFD).

Gestão de um certificado de Carimbo do Tempo: A emissão do certificado de carimbo do tempo é realizada por uma Autoridade de Carimbo do Tempo (TSA), que deve estar registrada junto à DGDCFD, cumprindo as regulamentações da "Política de carimbo do tempo do Sistema Nacional de Certificação Digital"

Gestão de um certificado de Pessoa Física e Pessoa jurídica: Os certificados de pessoa física e os certificados de pessoa jurídica são emitidos por uma Autoridade Certificadora autorizada ou registrada pelo MICITT.

Portanto, o Banco Central da Costa Rica tem constituída uma Autoridade Certificadora para a emissão de certificados de assinatura digital para pessoas físicas (CA SINPE - Pessoa Física) e outra para a emissão de certificados para pessoas jurídicas (CA SINPE- Pessoa Jurídica). Ambas as autoridades certificadoras pertencem à Hierarquia Nacional de Certificadores Registrados e estão devidamente inscritas e autorizadas a operar pela Diretoria de Certificadores de Assinatura Digital do Ministério de Ciência, Tecnologia e Telecomunicações (MICITT), órgão responsável pela administração e supervisão do Sistema Nacional de Certificação Digital.

Em outra ordem de ideias, a noção de interoperabilidade também será central para que os sistemas de informação dos parceiros possam se comunicar por meio de formatos de dados padronizados, como o XML, por exemplo, que se tornou indispensável nesse contexto. Essa linguagem permite modelar os processos, as trocas e garantir que seja estabelecida uma linguagem comum entre os diferentes atores.

Capítulo 3. O estabelecimento da administração eletrônica

A evolução da legislação relacionada com o direito provatório reconheceu o valor da evidência contida em documentos eletrônicos, refletindo assim a crescente importância dos meios digitais no âmbito legal e administrativo.

Este avanço é global e busca proporcionar a confiança jurídica necessária para impulsionar o comércio eletrônico em todos os países.

Como resultado, surge o que se conhece como administração eletrônica, marcando uma mudança rumo à virtualização dos processos comerciais. Esse processo geralmente começa com a implementação de transmissões e serviços online, seguido pela adoção da assinatura digital. Essa transformação implica a geração de documentos digitais que precisam ser preservados, assim como suas contrapartes em papel eram no passado

3.1. O desenvolvimento da administração eletrônica na Costa Rica

Na Costa Rica, o governo digital ou administração eletrônica tem sido impulsionado em diferentes momentos e, ao mesmo tempo, diferentes documentos foram gerados e/ou utilizados, conforme bem destaca Romero Pérez (2018) a seguir.

3.1.1. Reuniões internacionais:

- Carta Iberoamericana de Governo Eletrônico. Adotada pela XVII Cúpula Ibero-americana de Chefes de Estado e de Governo, Chile, novembro de 2007.
- Segunda conferência ministerial sobre a sociedade da Informação na América Latina e no Caribe, EL Salvador, fevereiro 2008.
- Carta Iberoamericana de qualidade da gestão pública. Adotada na XVIII Cúpula Ibero-americana de Chefes de Estado e de Governo, El Salvador, outubro de 2008.

3.1.2. Leis costarriquenhas:

- Nº. 7169 Promoção do desenvolvimento científico e tecnológico, 26 de junho de 1990
- Nº. 8220 Proteção ao cidadão contra o excesso de requisitos e trâmites administrativos 4 de março de 2002
- Nº. 8454 Certificados, assinaturas digitais e documentos eletrônicos 30 agosto 2005
- Nº. 9046 Transferência do setor de telecomunicações do Ministério do Meio Ambiente, Energia e Telecomunicações para o Ministério da Ciência e Tecnologia, 25 de julho 2012
- Nº. 9943 Criação da agência nacional de Governo Digital 11 de maio de 2021

3.1.3. Decretos Executivos:

- Nº. 31681 Criação da Comissão Nacional de Tecnologias da Informação e da Comunicação 20 janeiro 2004
- Nº. 33147 O Ministério da Presidência cria a Comissão Intersetorial de Governo Digital para elaborar e planejar políticas públicas nessa área. 8 de maio de 2006.
- Nº. 34093 de 10 de outubro de 2007 faz uma reforma na Comissão Intersetorial de Governo Digital.
- Nº. 34413 de 1de abril de 2008 Realiza uma reforma integral do Decreto Executivo Nº. 33147-MP que criou a Comissão Intersetorial de Governo Digital.
- Nº. 34702 de 6 de maio de 2008. Realiza uma reforma parcial nos artigos 2 e 4 do decreto executivo Nº 33147 citado
- Nº. 35139 Ministério da Presidência - Ministério do Planejamento Criação da Comissão Intersetorial de Governo Digital, a cargo do Ministério do Planejamento 6 de abril 2009
- Nº. 34704 Promoção do Teletrabalho nas Instituições Públicas 31 julho 2009
- Nº. 35776 Ministério do Planejamento- Governo e Justiça Promoção do modelo de interoperabilidade no setor público. 1 março 2010
- Nº. 36176 Ministério do Planejamento. Reforma do artigo 1 do decreto executivo Nº. 35139 4 outubro 2010.
- Nº. 38276 MIDEPLAN- MICITT de 18 de março de 2014 Promoção do governo aberto nas instituições públicas; e, criação da comissão intersetorial de governo aberto. (pp.161-163)

3.1.4. Outros documentos:

- O Plano Nacional de Ciência, Tecnologia e Inovação 2015-2021 (PNCTI) (Governo da Costa Rica, 2015) estabelece a incorporação do eixo de transformação digital nos projetos intersetoriais e propõe que, ao se pensar em uma grande temática como a inovação e modernização da gestão pública, dois são os elementos que podem contribuir para uma melhor gestão pública, tanto no nível do setor público centralizado e descentralizado, quanto no nível local ou municipal: governo aberto e governo eletrônico (Governo da Costa Rica, 2015).
- Política Nacional de Sociedade e Economia baseadas no Conhecimento (PNSEBC), que em seu quinto pilar de tecnologia digital, propõe o fomento das tecnologias digitais como catalisador do conhecimento. (Governo da Costa Rica, 2017).
- Diretriz 019-MP-MICITT Desenvolvimento do Governo Digital do Bicentenário, emitida en 21 de agosto de 2018.
- Estratégia de Transformação Digital rumo à Costa Rica do Bicentenário 4.0 (2018–2022), promovida pela Presidência e pelo Micitt.
- Regulamento do Expediente Eletrônico Único em Saúde, aprovado pela Diretoria da Caixa Costarriquenha de Seguro Social, na sessão 8954, realizada em 29 de janeiro de 2018.

Atualmente, na Costa Rica podem ser realizados trâmites com a assinatura digital certificada em 60 instituições públicas diferentes, de cerca de 350 que o Estado possui. (mifirmadigital, 2022).

No Índice de Desenvolvimento de Governo Digital da Organização das Nações Unidas (ONU), de 2021, a Costa Rica se posicionou pela primeira vez na seção de “Muito Alto Nível de Desenvolvimento de Governo Digital”, ocupando a 7ª posição nas Américas e a 56ª no ranking mundial.

Além disso, a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE, 2020) destaca avanços da Costa Rica em transformação digital que serão chave para acelerar a recuperação pós pandemia do COVID-19.

3.2. Aspectos da administração eletrônica

Os conceitos de administração eletrônica, governo aberto, governo digital e governo inteligente e sua interrelação encontram-se atualmente em pleno processo de debate e construção, não apenas na América Latina e no Caribe, mas também em todo o mundo.

O governo aberto tem como principais objetivos: i) melhorar os níveis de transparência e acesso à informação por meio da abertura de dados públicos (para exercer o controle social sobre os governos e exigir prestação de contas) e a reutilização das informações do setor público (para promover a inovação e o desenvolvimento econômico);
ii) facilitar a participação da cidadania no projeto e implementação das políticas públicas (e influenciar na tomada de decisões); e iii) favorecer a geração de espaços de colaboração e inovação entre os diversos atores, particularmente entre as administrações públicas, a sociedade civil e o setor privado, para co-desenhar ou co-produzir valor público, social e cívico. (Enriquez e Saénz, 2022, pp. 15).

Sobre o governo digital, suas áreas de ação são:

- Próximo: busca melhorar a interação entre os cidadãos e o Estado por meio de serviços de alta qualidade.

- Eficiente: desenvolve as bases dos sistemas de gestão que simplificam e unificam os processos transversais a cada organismo do Estado para que ofereça melhores serviços.
- Inteligente: aproveita os dados, informações e conhecimento como ativos de governo para otimizar os serviços públicos, oferecer experiências de serviços integrados e proativos, fortalecer a interação com o cidadão e a cocriação de políticas públicas.
- Integrado: busca a integração tecnológica entre os diferentes organismos do Estado, assim como a integração entre o Estado, a cidadania, a indústria e a academia. Potência a integração tecnológica e a interoperabilidade dos dados como base do desenvolvimento e a evolução dos sistemas de gestão.
- Confiável: zela por responder aos riscos, ameaças e desafios que surgem com o desenvolvimento das tecnologias digitais. Foca em gerar e disponibilizar estruturas que proporcionem segurança e confiança na aplicação e evolução do governo digital. (Enríquez e Sáenz, 2022, pp. 15)

Para isso, são necessários elementos como a interoperabilidade e a segurança das transações virtuais.

COMPLEMENTO

No site Pura Vida Digital (2018-2022), é possível encontrar diversos serviços voltados ao cidadão que podem ser realizados à distância.

https://www.gob.go.cr/

3.3. A questão da interoperabilidade para o arquivo

O que é importante lembrar?

A **interoperabilidade** se traduz concretamente na capacidade das entidades administrativas, dotadas de aplicações informáticas, **de trocar dados e serviços** com outras entidades ou com os cidadãos.

Isso implica, por exemplo, poder criar, administrar e transmitir dados a partir de uma aplicação A, que roda em um sistema operacional específico e em um computador determinado, e reutilizar esses dados em uma aplicação local B ou remota, operando no mesmo ou em outro sistema operacional e geralmente em outro computador. Cada um desses dois contextos técnicos pode evoluir de forma independente, conforme várias limitações

Para tornar isso possível em um **marco de múltiplas entidades** que trocam informações de forma digital, é necessário:

- que a estrutura de dados seja neutral e independente de uma aplicação ou pacote de software em particular.
- que a descrição destes dados seja uma descrição padronizada, reconhecida pelas diferentes entidades e usuários.

Essas duas orientações técnicas, motivadas pela necessidade de interoperabilidade, facilitam enormemente o arquivamento dessas informações.

Para ser interoperável, como foi mostrado, é necessário manter-se neutro em relação a uma aplicação específica e padronizar a descrição dos dados, conforme apontam Franco Espiño e Pérez Alcazar (2014) no *Modelo de Gestão de Documentos e Administração de Arquivos* (MGD) para a Rede de Transparência e Acesso à Informação (RTA), promovida pela União Europeia, como requisitos essenciais no design da arquitetura e de uma plataforma de interoperabilidade na região, destacam-se os seguintes:

Não centralidade. Para permitir uma adaptação dos componentes das plataformas às características dos sistemas de informação já existentes e respeitar a autonomia dos países e regiões para estabelecer regras internas de funcionalidade.

Bens públicos regionais. Para preservar os direitos de propriedade e uso da solução de interoperabilidade como patrimônio comum de conhecimento, evitando o uso de patentes privadas.

Cooperação e reutilização. Para possibilitar que cada país participante desse estudo de pesquisa avance, com os menores custos e esforços possíveis, no processo de automação e interoperabilidade.

Mecanismos de consenso para definir e adotar padrões. Para outorgar um valor formal à definição de padrões, mediante prévio consenso, e gerar confiança. (pp.8)

3.4. Dimensões da interoperabilidade

Quanto à interoperabilidade, é comumente aceito referir-se a três dimensões: técnica, semântica e organizacional, contudo, segundo (Franco Espiño e Pérez Alcazar, 2014), ao falar sobre gestão de documentos e administração de arquivos, é oportuno enfatizar a necessidade de compreender a interoperabilidade sob outra dimensão, que é a sua durabilidade ou permanência ao longo do tempo.

- I**nteroperabilidade técnica.** Referida à garantia de que os componentes tecnológicos estão preparados para a colaboração. É a dimensão que deve permitir mecanismos comuns de transferência de dados.
- **Interoperabilidade semântica.** Referida à garantia de que o significado da informação possa ser compreendido por qualquer aplicação. É a dimensão que habilita os sistemas a combinar informações de fontes externas e processá-las adequadamente.
- **Interoperabilidade organizativa.** Referida à garantia da colaboração entre as organizações que desejam trocar informações. É a dimensão que assegura a coordenação e o alinhamento dos procedimentos envolvidos na prestação de serviços.
- **Interoperabilidade no tempo.** Referida à garantia de interação entre elementos que correspondam a diferentes gerações tecnológicas. É a dimensão que assegura a adequada recuperação e conservação da informação em suporte eletrônico. (pp. 9)

A interoperabilidade no tempo é um domínio que consta no Esquema Nacional de Interoperabilidade, aprovado em 2010 pelo Governo da Espanha.

EXEMPLO

Os padrões abertos garantem e facilitam a interoperabilidade. São desenvolvidos em um processo transparente e colaborativo, estão disponíveis de forma gratuita ou a um custo razoável, e podem ser implementados por particulares. Alguns exemplos de padrões abertos são: TCP/IP, HTTP, HTML, ODF, JSON RESTful, Oauth, etc.

COMPLEMENTO

Para mais informações, você pode consultar as regulamentações e diretrizes emitidas pelo Governo da Espanha, como parte do Esquema Nacional de Interoperabilidade. Por exemplo: o Guia de Aplicação da Norma Técnica de Interoperabilidade para Documento Eletrônico e o Manual do Usuário "Esquemas XML para a troca de documentos eletrônicos e processos eletrônicos".

Disponível em https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html

3.5. Conceito de autenticidade em um ambiente digital: trabalho do grupo InterPARES

Este grupo de trabalho interdisciplinar, sediado na Universidade da British Columbia e liderado pela professora Luciana Duranti, buscou inicialmente (InterPARES 1, 1999-2002) definir as regras e princípios necessários para demonstrar que um documento digital possui caráter de autenticidade.

Ao longo do tempo, foram desenvolvidos vários projetos InterPARES (fases: 2, 3 e 4), este último InterPARES Trust chamado Itrust (2012-2019), consistiu em um "projeto de pesquisa interdisciplinar multinacional que explora questões de confiança e confiabilidade dos registros e dados em ambientes online

Seu objetivo é gerar os marcos teóricos e metodológicos para desenvolver políticas, procedimentos, regulamentos, normas e legislações locais, nacionais e internacionais, a fim de garantir a confiança dos cidadãos baseada em evidências de boa governança, uma economia digital forte e uma memória digital persistente.

ITrust é uma associação de pesquisa que reúne mais de cinquenta universidades e organizações, nacionais e multinacionais, públicas e privadas, na América do Norte, América Latina, Europa, África, Australásia e Ásia (a Aliança Internacional). Os pesquisadores são especialistas em arquivologia, gestão de registros, diplomacia, direito, tecnologia da informação, comunicação e mídia, jornalismo, comércio eletrônico, informática em saúde, cibersegurança, governança e garantia da informação, análise forense digital, engenharia de computação e política da informação.

(InterPARES 3 Proyect, 2022) possui uma base de dados terminológica do projeto, da qual se extrai o significado para este trabalho dos termos 'autêntico' e 'autenticidade', conforme detalhado a seguir:

autêntico

Juntamente com confiança e exatidão, é um dos elementos que constituem a confiabilidade de um documento arquivístico; consiste na certificação de que um documento arquivístico é aquilo que pretende ser, sem alterações ou corrupções. Os documentos autênticos são aqueles que mantiveram sua identidade e integridade ao longo do tempo, graças à evidência de seu caráter, requisitos ou circunstâncias inerentes. *(Ver também: autenticação, avaliação de autenticidade , presunção de autenticidade , requisito de autenticidade , requisitos básicos de autenticidade, requisitos de referência)*

Termos traduzidos:

autenticidade

s., A confiabilidade de um registro enquanto registro; ou seja, a qualidade de um registro que é aquilo que pretende ser e que está livre de manipulação ou corrupção. *(Ver também:* a*valiação da autenticidade , autenticação, requisito de autenticidade*
, *requisitos de autenticidade de referência , requisitos de autenticidade de referência , presunção de autenticidade,) n., A* qualidade de ser autêntico, ou com direito a aceitação. Por estar autorizado ou devidamente autorizado, por ser aquilo que afirma ser na origem ou autoria, por ser genuíno. 1Requisitos de referência que sustentam a produção de cópias autênticas de registros eletrônicos: as condições mínimas necessárias para permitir que o conservador certifique a autenticidade das cópias de registros eletrônicos. Requisitos de referência que sustentam a presunção de autenticidade dos registros eletrônicos: as condições que servem como base para a avaliação da autenticidade dos registros eletrônicos pelo conservador. (parágrafos 1-2)

COMPLEMENTO

As extensas pesquisas realizadas durante o InterPARES 1, ao longo de três anos, nesse contexto resultaram na definição de um conjunto de catorze princípios e critérios.

1. Tratar os documentos de arquivo de uma maneira específica em vez de considerá-los como objetos digitalizados em geral; isto é, tratá-los como documentos criados ou recebidos e classificados no exercício das atividades laborais.
2. Focar em documentos arquivísticos eletrônicos autênticos: Um documento arquivístico eletrônico genuíno é um documento que é aquilo que deve ser e que está livre de alterações ou modificações. Portanto, comprovar a autenticidade de um documento arquivístico eletrônico implica estabelecer sua identidade e demonstrar sua integridade com base em condições de referência e condições mínimas de autenticidade. Quando se trata de um registro arquivístico eletrônico, considera-se que ele está essencialmente completo e inalterado se a mensagem que pretende transmitir para cumprir seu propósito não for modificada.

3. Reconhecer e levar em consideração que o maior risco para a autenticidade dos documentos arquivísticos eletrônicos ocorre durante sua transmissão no espaço (por exemplo, a transmissão entre pessoas, sistemas ou programas de aplicação) ou no tempo (por exemplo, quando são armazenados offline ou quando o hardware ou software utilizado para seu processamento, comunicação ou manutenção é atualizado ou substituído).
4. Reconhecer que a preservação de documentos arquivísticos eletrônicos autênticos é um processo contínuo que começa com sua criação e cujo objetivo é a transmissão de documentos arquivísticos eletrônicos autênticos no espaço e no tempo (cadeia de custódia ininterrupta).
5. Basear-se no conceito de confiabilidade na manutenção e preservação de documentos arquivísticos, e especificamente no conceito de um sistema confiável de gestão de documentos arquivísticos e no papel do custodiante como um repositório confiável.
6. Basear-se no reconhecimento de que não é possível preservar um documento arquivístico eletrônico da mesma forma que um objeto físico armazenado; só podemos preservar a capacidade de reproduzi-lo.
7. Reconhecer que os elementos constitutivos físicos e intelectuais de um documento arquivístico eletrônico não precisam, necessariamente, coincidir e que o conceito de elemento constitutivo digital é distinto do conceito de elemento de forma documental.
8. Especificar as condições necessárias para que uma cópia de um documento arquivístico eletrônico seja considerada equivalente ao original: em princípio, o original de um documento arquivístico eletrônico é o primeiro documento completo e efetivo. Entretanto, no ambiente eletrônico, nenhum documento sobrevive na sua forma original. Qualquer cópia que seja fiel ao conteúdo e à forma documental do original deve ser considerada como uma cópia fiel do original, equivalente ao original no que diz respeito às suas consequências. Qualquer cópia certificada como autêntica por um agente a quem tenha sido confiada essa responsabilidade é tão válida quanto o original.
9. Integrar a avaliação dos documentos arquivísticos eletrônicos no processo contínuo de preservação.
10. Integrar a descrição arquivística no processo contínuo de preservação: a descrição arquivística deve fornecer uma certificação geral da autenticidade dos documentos arquivísticos eletrônicos e de sua relação com outros documentos no contexto do fundo ao qual pertencem, seguindo as condições mínimas exigidas.
11. Indicar explicitamente que o processo de conservação deve estar completamente documentado, como meio principal de proteção e avaliação da autenticidade a longo prazo.
12. Reconhecer explicitamente que o princípio tradicional da presunção de autenticidade dos documentos arquivísticos utilizados no curso normal das atividades comerciais deve ser acompanhado, no caso dos documentos arquivísticos eletrônicos, da prova de que não foram manipulados de forma inadequada.
13. Reconhecer que o responsável deve avaliar como manter a autenticidade dos documentos de arquivo eletrônicos. A avaliação da autenticidade dos documentos é realizada antes de sua transferência ao custodiante e faz parte do processo de avaliação, enquanto a manutenção da autenticidade das cópias dos documentos ocorre após a transferência, como parte do processo de preservação a longo prazo.
14. Fazer uma distinção clara entre a proteção da autenticidade dos documentos do arquivo digital e a autenticação do documento.

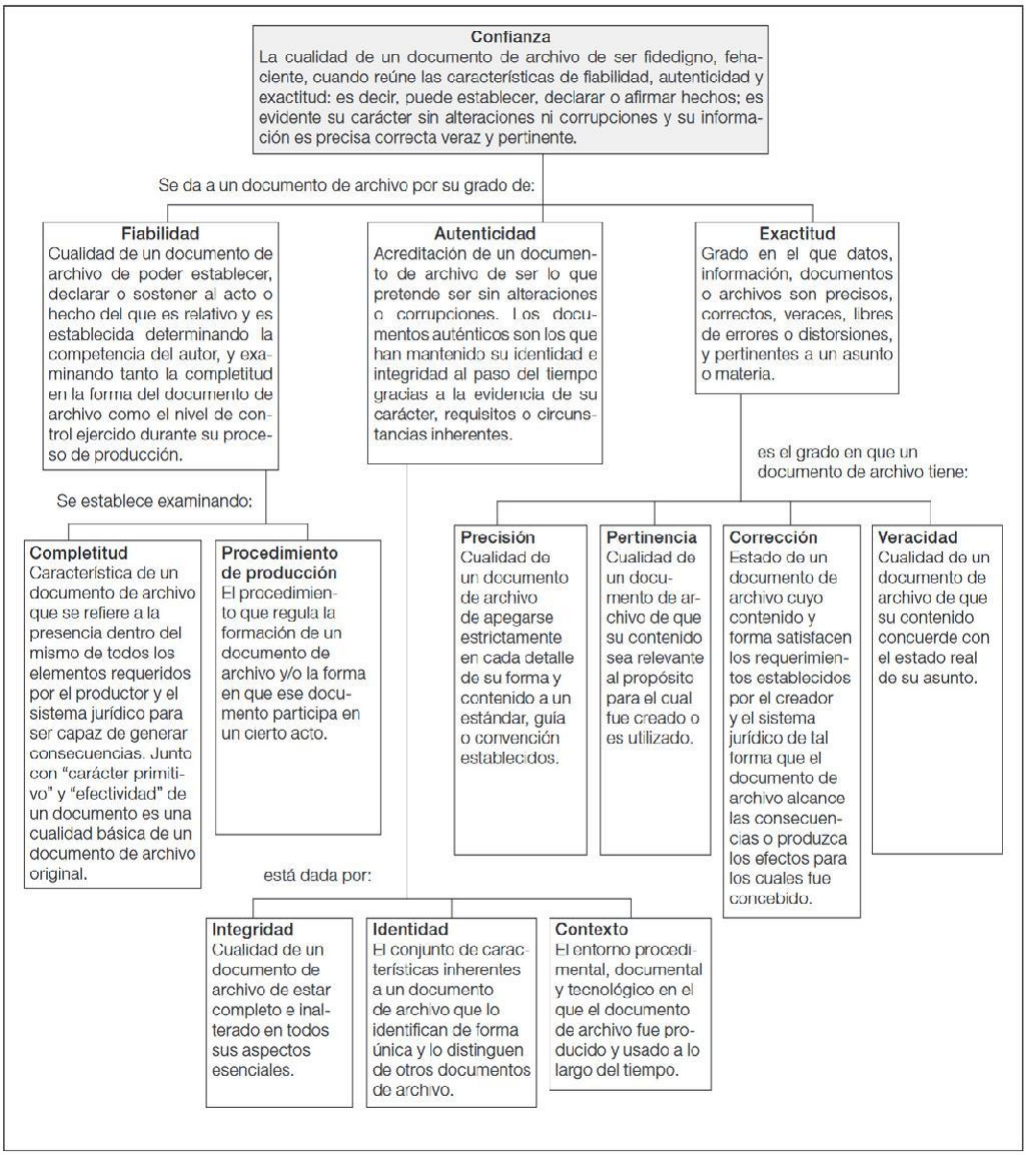
Atualmente, os desafios de resguardar documentos na nuvem também apresentam novos desafios para os arquivistas, pois a preservação digital se tornou um serviço a ser oferecido para muitos setores.

Segundo Thibodeau et al. (2017) referente à Preservação como serviço de confiança conhecido por suas siglas PaaST, menciona que este apresenta requisitos funcionais e de dados para a preservação digital, além disso, amplia os achados dos anteriores projetos InterPARES de duas maneiras. Em primeiro lugar, a pesquisa do InterPARES tem se concentrado em documentos digitais, mas os requisitos do PaaST foram formulados para serem aplicáveis à preservação de praticamente qualquer tipo de informação digital, não apenas documentos. Em segundo lugar, embora o tratamento anterior da preservação no InterPARES fosse abstrato e conceitual, os requisitos do PaaST são formulados para apoiar a implementação e até a produção de software para preservação.

Segundo o PaaST, a autenticidade é "a capacidade de um Registro de comunicar a mensagem que se pretendia fornecer no contexto em que foi um Registro" (p.66), e está relacionada ao mesmo tempo com "Uma avaliação da autenticidade nos permite determinar se a possibilidade de reconhecer o significado de um Registro foi afetada pelo passar do tempo. Idealmente, não deveria ser" (p.66).

Dessa maneira, autenticidade e preservação estão vinculadas, pois uma adequada preservação digital permitirá conservar a autenticidade do documento. Ao mesmo tempo, o InterPARES PaaST fornece listas de verificação de aspectos de preservação e autenticidade com as quais se pode manter um ambiente adequado de conservação, no qual o ambiente é visto como um todo que:

> inclui tanto o conjunto de Objetivos de Preservação que são mantidos sob as mesmas Normas de Conservação quanto as infraestruturas tecnológicas e ferramentas utilizadas na sua conservação. O Ambiente de Preservação pode incluir hardware e software separados, diferentes e independentes, utilizados por diferentes Provedores de Serviços de Preservação. As capacidades oferecidas por um único provedor são denominadas Ambiente de Preservação Local. (p.2)



ONTOLOGIA. Confiança em um documento de arquivo. Elaborado por Banard A, Voutssas J, 2014, no Glossário de Preservação Arquivística Digital. P. 231

3.6. Arquivar em planos governamentais

É importante que os governos planejem ações específicas para o arquivo digital e eletrônico, no caso da Costa Rica, essas ações estão contempladas na Lei 8454, que é o principal marco normativo da assinatura digital, certificados e documentos eletrônicos esses documentos, além disso, devem ser protegidos conforme a Lei 7202 do Sistema Nacional de Arquivos, ligando e complementando ambas as normas, razão pela qual não podem ser vistas de forma independente uma da outra.

CONSELHO: MODELO OAIS E OS PADRÕES ASSOCIADOS

O Modelo de Referência OAIS: Sistema de Informação de Arquivo Aberto é atualmente uma norma ISO. Entretanto, foi originalmente desenvolvida pelo *Consultative Committee for Space Data Systems* (ccsds), um grupo de trabalho das agências espaciais a nível mundial, focado em dados terrestres e espaciais, com o objetivo de se constituir como um **modelo de referência** que definisse os processos necessários para preservar e acessar os objetos de informação de forma eficaz e a longo prazo, além de estabelecer uma linguagem comum que os descreva, entre outros aspectos, para a preservação da informação como apontam Cruz Mundet e Díez Carrera (2014) "As funções das quais se ocupa são: o ingresso, a instalação, a gestão de dados, o acesso e a difusão; ou seja, todo o ciclo de vida da preservação digital" (p.132).

Além disso, existem outros modelos de preservação digital, tais como: PREMIS para metadados, OAIS, DAMM fornece uma forma de categorizar diferentes abordagens para permitir que as organizações compreendam as diferenças e selecionem a melhor solução para elas em termos de preservação da informação, o DoD.5015.2, que por sua vez deriva de padrões criados na Universidade da Colúmbia Britânica no Canadá. MoReq (Modelo de requisitos para a gestão de documentos de arquivo), que, sem ser um modelo de preservação, é chamativo já que abrange aspectos que são úteis para a mesma.

Além disso, na Austrália foi criado um modelo conhecido como "Records Continuum" (Contínuo dos documentos de arquivo), wsse modelo se opõe ao mais utilizado, baseado no conceito do "ciclo de vida" dos documentos de arquivo. O modelo do *records continuum* propõe que a gestão do documento é um processo contínuo desde o momento da sua criação e os conceitos relativos a tal gestão pertencem a quatro "dimensões"

Por sua vez, o InterPARES trabalhou em um modelo de abordagem para a preservação digital denominado "Cadeia de Preservação" (Chain of Preservation), que estabelece que os documentos de arquivo digitais devem ser cuidadosamente manuseados ao longo de toda a sua existência para garantir que sejam acessíveis e legíveis ao longo do tempo (Barnard Amozorrutia, 2013).

ATENÇÃO

Nem todos os sistemas requerem as mesmas necessidades de arquivo, daí a definição de um nível mínimo e um nível superior (requisitos adicionais) em termos de durabilidade, integridade e segurança.

Bibliografia

Asamblea Legislativa. (2005, octubre 13). Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55666&nValor3=60993&strTipM=TC

Asamblea Legislativa. (2021, setiembre 9). Ley sobre letra de cambio y pagaré electrónicos. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_articulo.aspx?param1=NRA&nValor1=1&nValor2=95870&nValor3=128143&nValor5=3&strTipM=FA

BANAT-BERGER F., HUC C., DUPLOUY L., *L'Archivage numérique à long terme, les débuts de la maturité?* (Primera obra de síntesis sobre el archivo digital en lengua francesa) Paris, La Documentation française, 2009

BANAT-BERGER F., HUC C., Module 7 - Gestion et archivage des documents numériques. Portail International Archivistique Francophone. 2011. https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques (Se identifica en el texto como PIAF)

Barnard, A y Voutssas, J (2014). Glosario de Preservación Archivística Digital Versión 4.0. Universidad Nacional Autónoma de México. https://iibi.unam.mx/archivistica/glosario_preservacion_archivistica_digital_v4.0.pdf

Barnard Amozorrutia, A. (. (2013). Archivos electrónicos.Textos y contextos II. Puebla, México: Universidad Autónoma de Puebla. Recuperado de http://www.interpares.org/display_file.cfm?doc=ip3_mexico_dissemination_bc_ barnard-et_al_archivos-electr%C3%B3nicos_2013.pdf

Cruz Mundet, J. R., y Díez Carrera, C. (2014). La normalización dela preservación digital permanente: análisis del modelo de referencia OAIS. Revista del Archivo Nacional, 129-154. Recuperado de http://www.dgan.go.cr/ran/ index.php/RAN/article/view/91/45

Enriquez, A., y Saénz, C. (2022). Gobierno digital. Pieza clave para la consolidación de estados democráticos en los países del SICA. Recuperado de https://repositorio.cepal.org/bitstream/handle/11362/47811/1/S2200164_es.pdf

Franco Espiño, B., y Pérez Alcazar, R. (2014). Directrices –Interoperabilidad. Modelo de Gestión de Documentos y Administración de Archivos (MGD) para la Red de transparencia y Acceso a la Información (RTA). Recuperado de https://www.archivonacional.go.cr/web/dsae/administracion_electronica_interoperabilidad.pdf

InterPARES Proyect. (2022, octubre 21). Auténtico y autenticidad. Recuperado de http://www.interpares.org/ip3/ip3_terminology_db.cfm?team=15

mifirmadigital. (2022, octubre 21). *¿Qué puedo hacer?* Recuperado de https://www.mifirmadigital.go.cr/

Ministerio de Ciencia, Tecnología y Telecomunicaciones MICITT. (2013, mayo 20). Política de Certificados para la Jerarquía Nacional de Certificadores Registrados. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74874&nValor3=92603&strTipM=TC

Organización de las Naciones Unidas ONU. (2021). Índice de Desarrollo. Récupéré sur https://www.un.org/es/

Organización para la cooperación y el Desarrollo Económico OCDE. (2020). Informe sobre las Perspectivas Económicas de América Latina. Recuperado de https://www.comex.go.cr/sala-de-prensa/comunicados/2020/octubre/cp-2534-ocde-destaca-avances-de-costa-rica-en-transformaci%C3%B3n-digital/

Poder Ejecutivo. (2006, abril 21). Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 33018. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=56884&nValor3=103000&strTipM=TC

Presidencia (2022, octubre 21). Costa Rica lanza Agencia Nacional de Gobierno Digital Recuperado de https://www. presidencia.go.cr/comunicados/2021/11/costa-rica-lanza-agencia-nacional-de-gobierno-digital/#:~:text=En%20el%20%C3%BAltimo%20%C3%ADndice%20de,y%20%2356%20a%20nivel%20mundial

Pura vida digital. (2018-2022). https://repositorio.cepal.org/bitstream/handle/11362/47811/1/S2200164_es.pdf.

Romero Pérez, J. E. (2018). La administración electrónica pública. Revista de Ciencias Jurídicas (149), 105-132. Recuperado de https://revistas.ucr.ac.cr/index.php/juridicas/article/download/39570/40111/

Sistema Costarricense de Información Jurídica SINALEVI. (2022, octubre 21). SCIJ Sistema Costarricense de Información Jurídica. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55666&nValor3=60993&strTipM=TC

Thibodeau, K. et al. (2017). Preservación como servicio de confianza (PaaST). Requisitos funcionales y de datos para la preservación digital. InterPARES TRUST. Recuperado de http://interparestrust.org/assets/public/dissemination/PreservationasaServiceforTrust1_0.pdf?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wapp&_x_tr_sch=http

Est ora maximus patu vivastr idinte dicae iam hui crissum intium escerumur im hinatiquis, scere, movidetis Mulvist fue culiam faus, Ti. Viverterta partant ervis, quam dem occiisquam rehenes traves con Etre temunum is cont Cate caperit. Scierortum hem publicaper hil vidiu ia crectus sedeferet vil halis maximmo rbitrat uussoltus inculius num orurnum vid contesimis. Opio, patus, con sulicae non sum ium consum quam iac reistri puliissum mactum senirit; iam diem, ius. At et nestem det Cat es in dendiem terfirmis iu inatimis rei ilin sed num tiquam ciensup erioret videm hinprit, claribus sentem, Cas omner inat.

Ceressa pra o hactus ta popublica de con dien Ita menatam, novideme mo ina, comne is re fora, consitant, comaximil hordin serfes acienica; C. Tam misquit? Patus; et? Nihicat orudam potis nost achum et? Mulius, dium ena, pro, nulutertam loc vervica ucont.

Lium iurenih ilius, ubitiss enterei convo, quam ad det; inat, Cupiestilius patissum tum or larbis strobsentua novignos, cone dum vit cerum orte interum opublin tiocus omantem diem nors inveri potalar idemei fatiam eto cae consulv idelum incur. Grae confeci puline cres cidiis eo, pubis orteriorunte im orte in serbis, se rei cone que entis; nos C. Ridem turi, spio pul tes vilnemquo iu vastenatio num et furbefa cerceri ssulos patide quam areo et, que ego con nitis conem inatque egerat, quid sus hocam et ac faci pultum pos essulici et, faudam nihin vit. Vivit? iam. Eperter befectum pes coticon susatim esissum quides et L. Hocrum menatum dem in se inatumus verehemquam nius deribus sum haleris verum opultuam intimore ericatu ssimilius consultum eo vidiurore, no. Lus esse mortusu lissultum etraetis. M. Rae terdiis trumur inprox num, fac recondam omnit.

Ehebatumusa remum ta Sci postro iam cae num ati, Cat, nosside licitam propopo publibus es porae ac ta cre cons Ad potistinat, perede tiente, cris. Iquossul hosus, quod C. Adduc rem P. Nihilie millesi gnatili, nernihica; C. Batam, que adhucon sulabessici spio cae, nos Ahacrus cone esum is hocciem in senterione aperracia L. Habeffreis;


IBERARCHIVOS
IBERARQUIVOS


ARCHIVO NACIONAL
COSTA RICA


UNIVERSIDAD DE
COSTA RICA