www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v.30, n.162, 2026 | DOI: 10.69849/a3jk6x51

Integração de soluções de assinatura eletrônica e conformidade fiscal (Document and Reporting Compliance — DRC) em ambientes SAP S/4HANA globais: uma abordagem histórica, técnica e evolutiva

Integration of electronic signature and fiscal compliance solutions (Document and Reporting Compliance — DRC) in global SAP S/4HANA environments: a historical, technical and evolutionary approach

François Pierre Fagundes Francelino

RESUMO

Este artigo tem por objetivo analisar, sob uma perspectiva histórica e evolutiva, a integração entre soluções de assinatura eletrônica e mecanismos de conformidade fiscal digital — notadamente o SAP Document and Reporting Compliance (SAP DRC) — em ambientes corporativos baseados em SAP S/4HANA operando em múltiplas jurisdições. Parte-se da premissa de que a digitalização das obrigações fiscais acessórias e a consolidação de infraestruturas de chave pública (PKI) constituem processos convergentes, cuja trajetória remonta às primeiras legislações sobre comércio eletrônico da década de 1990 e se estende até os modelos contemporâneos de controle contínuo de transações (Continuous Transaction Controls — CTC) adotados por autoridades tributárias em dezenas de países. A pesquisa, de natureza bibliográfica e documental, examina a evolução normativa internacional (UNCITRAL, eIDAS, ESIGN Act/UETA) e nacional (Medida Provisória nº 2.200-2/2001, Lei nº 14.063/2020, modelo ICP-Brasil), correlacionando-a com a evolução arquitetural das soluções SAP para documentos eletrônicos, do extinto SAP NF-e ao atual eDocument Framework e à plataforma SAP Document and Reporting Compliance sobre o SAP Business Technology Platform (SAP BTP). Discutem-se os padrões técnicos de assinatura digital em documentos eletrônicos (XAdES, PAdES, CAdES), os modelos de integração via Application Interface Framework (AIF) e SAP Cloud Connector, bem como os principais desafios técnicos, jurídicos e de segurança

da informação enfrentados por corporações multinacionais na padronização global associada à conformidade local — princípio sintetizado pela SAP como "standardize globally, comply locally". Conclui-se que a maturidade da integração entre assinatura eletrônica e DRC em S/4HANA depende de arquiteturas modulares, orientadas a APIs, capazes de absorver mudanças regulatórias frequentes sem comprometer a integridade e a rastreabilidade das transações fiscais eletrônicas.

Palavras-chave: Assinatura Eletrônica. Conformidade Fiscal Digital. SAP S/4HANA. Document and Reporting Compliance. Infraestrutura de Chaves Públicas. eIDAS. ICP-Brasil. eDocument Framework.

ABSTRACT

This article analyzes, from a historical and evolutionary perspective, the integration between electronic signature solutions and digital fiscal compliance mechanisms — particularly SAP Document and Reporting Compliance (SAP DRC) — within corporate environments based on SAP S/4HANA operating across multiple jurisdictions. It is assumed that the digitalization of ancillary tax obligations and the consolidation of public key infrastructures (PKI) are convergent processes whose trajectory dates back to the earliest e-commerce statutes of the 1990s and extends to contemporary Continuous Transaction Controls (CTC) models adopted by tax authorities in dozens of countries. This bibliographic and documentary study examines international regulatory evolution (UNCITRAL, eIDAS, ESIGN Act/UETA) and Brazilian regulation (Provisional Measure No. 2,200-2/2001, Law No. 14,063/2020, the ICP-Brasil trust model), correlating it with the architectural evolution of SAP electronic-document solutions, from the discontinued SAP NF-e to the current eDocument Framework and the SAP Document and Reporting Compliance platform on SAP Business Technology Platform (SAP BTP). Technical digital-signature standards for electronic documents (XAdES, PAdES, CAdES), integration models via the Application Interface Framework (AIF) and SAP Cloud Connector, and the principal technical, legal and information-security challenges faced by multinational corporations in reconciling global standardization with local compliance are discussed — a principle summarized by SAP as "standardize globally,

comply locally". The study concludes that mature integration between electronic signature and DRC in S/4HANA depends on modular, API-oriented architectures capable of absorbing frequent regulatory change without compromising the integrity and traceability of electronic fiscal transactions.

Keywords: Electronic Signature. Digital Fiscal Compliance. SAP S/4HANA. Document and Reporting Compliance. Public Key Infrastructure. eIDAS. ICP-Brasil. eDocument Framework.

1 INTRODUÇÃO

A digitalização das relações econômicas transformou, ao longo das três últimas décadas, tanto a forma pela qual as partes manifestam consentimento em transações jurídicas quanto a forma pela qual o Estado fiscaliza e arrecada tributos incidentes sobre tais transações. Duas trajetórias tecnológicas e regulatórias, originalmente distintas, convergiram progressivamente: de um lado, a assinatura eletrônica, fundamentada em criptografia assimétrica e infraestruturas de chave pública (Public Key Infrastructure — PKI); de outro, a conformidade fiscal digital, materializada em documentos fiscais eletrônicos, obrigações acessórias digitais e modelos de controle contínuo de transações (Continuous Transaction Controls — CTC) exercidos por administrações tributárias.

Em ambientes corporativos de grande porte, essa convergência encontra expressão concreta nos sistemas de Enterprise Resource Planning (ERP), notadamente na suíte SAP S/4HANA, na qual o módulo SAP Document and Reporting Compliance (SAP DRC) centraliza a criação, a assinatura, a transmissão, o monitoramento e o arquivamento de documentos fiscais eletrônicos em mais de cinquenta países (SAP SE, 2024). A operação de corporações multinacionais sob um único ambiente S/4HANA global impõe o desafio de compatibilizar um núcleo de processos padronizado (core global template) com exigências jurídicas, técnicas e criptográficas absolutamente distintas entre jurisdições — desafio que a própria SAP sintetiza no princípio "standardize globally, comply locally" (padronizar globalmente, estar em conformidade localmente).

O presente artigo tem como objetivo geral investigar, sob uma perspectiva histórica e evolutiva, a integração entre soluções de assinatura eletrônica e mecanismos de conformidade fiscal digital em ambientes SAP S/4HANA globais. Como objetivos específicos, busca-se: (i) reconstituir a trajetória normativa e tecnológica que conduziu da assinatura manuscrita à assinatura eletrônica qualificada; (ii) analisar a evolução arquitetural das soluções SAP voltadas a documentos eletrônicos e conformidade fiscal, do SAP NF-e ao SAP DRC; (iii) descrever os padrões técnicos e os modelos de integração empregados na assinatura digital de documentos fiscais eletrônicos dentro do ecossistema SAP; e (iv) discutir criticamente os desafios técnicos, jurídicos e de segurança da informação enfrentados por organizações globais nesse processo de integração.

Justifica-se a relevância do tema pela intensificação, observada sobretudo a partir de 2018, da adoção de mandatos de e-invoicing e de controles fiscais em tempo real por administrações tributárias ao redor do mundo — movimento impulsionado pela busca de redução do hiato tributário (tax gap), pela digitalização acelerada pós-pandemia de covid-19 e, mais recentemente, pelo pacote europeu "VAT in the Digital Age" (ViDA), formalmente adotado em março de 2025 e com implementação escalonada até 2035 (INNOWISE, 2026). Nesse cenário, compreender a arquitetura técnica e o arcabouço jurídico que sustentam a assinatura eletrônica de documentos fiscais deixa de ser tema de interesse meramente operacional para constituir-se em fator crítico de continuidade de negócios, de gestão de risco tributário e de governança corporativa.

Metodologicamente, o estudo adota abordagem qualitativa, de natureza bibliográfica e documental, com levantamento de fontes primárias — textos normativos nacionais e internacionais, normas técnicas ETSI e ISO, documentação oficial da SAP SE — e fontes secundárias especializadas em direito digital e em arquitetura de sistemas ERP. A análise é conduzida em perspectiva histórico-evolutiva, isto é, buscando reconstituir marcos temporais e relações de causalidade entre inovações regulatórias e inovações tecnológicas, sem prejuízo de uma discussão técnica aprofundada sobre a arquitetura corrente do SAP DRC em ambientes S/4HANA.

O artigo está estruturado em sete seções, além desta introdução. A seção 2 apresenta a fundamentação teórica e a evolução histórica da assinatura eletrônica e da documentação fiscal eletrônica. A seção 3 descreve a arquitetura do SAP DRC em S/4HANA. A seção 4 analisa a integração de assinatura eletrônica nesse ambiente. A seção 5 discute desafios e tendências. A seção 6 apresenta a metodologia empregada de forma consolidada. A seção 7 traz as considerações finais, seguidas das referências.

2 FUNDAMENTAÇÃO TEÓRICA E EVOLUÇÃO HISTÓRICA

2.1 Das origens da criptografia de chave pública à assinatura eletrônica

O conceito técnico que hoje sustenta a assinatura eletrônica tem origem na criptografia assimétrica, formalizada por Diffie e Hellman (1976) e posteriormente operacionalizada pelo algoritmo RSA, de Rivest, Shamir e Adleman (1978). O princípio é conhecido: um par de chaves matematicamente relacionadas — uma privada, mantida em sigilo pelo signatário, e outra pública, disponibilizada a terceiros — permite que uma mensagem cifrada com a chave privada seja verificada com a chave pública correspondente, atestando autoria e integridade sem revelar o segredo criptográfico. Esse mecanismo, originalmente concebido para sigilo de comunicações, revelou-se igualmente apto a cumprir a função jurídica da assinatura: autenticação do signatário e vinculação inequívoca ao conteúdo assinado.

A maturação técnica desse modelo exigiu, ainda, um componente organizacional: a infraestrutura de chaves públicas (PKI), estrutura hierárquica de Autoridades Certificadoras (AC) responsáveis por emitir, validar e revogar certificados digitais que associam uma chave pública a uma identidade verificada. O padrão X.509, da União Internacional de Telecomunicações, tornou-se a referência técnica dominante para certificados digitais a partir da década de 1990, sendo posteriormente incorporado, com adaptações nacionais, a praticamente todos os modelos regulatórios de assinatura eletrônica qualificada hoje vigentes.

2.2 Marcos regulatórios internacionais da assinatura eletrônica

O reconhecimento jurídico da assinatura eletrônica não decorreu automaticamente da disponibilidade técnica da criptografia assimétrica; exigiu construção normativa específica, tendo em vista o princípio da equivalência funcional entre o documento eletrônico e o documento em suporte físico. A Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL) exerceu papel pioneiro nesse processo, publicando em 1996 a Lei Modelo sobre Comércio Eletrônico e, em 2001, a Lei Modelo sobre Assinaturas Eletrônicas, ambas destinadas a orientar legislações nacionais segundo os princípios da neutralidade tecnológica, da equivalência funcional e da autonomia da vontade (UNCITRAL, 2001).

Nos Estados Unidos, esse movimento consolidou-se com o Uniform Electronic Transactions Act (UETA), de 1999, adotado pela quase totalidade dos estados americanos, e com a legislação federal Electronic Signatures in Global and National Commerce Act (ESIGN Act), sancionada em 2000, que conferiu validade jurídica a assinaturas e registros eletrônicos em transações interestaduais, adotando modelo amplamente tecnologicamente neutro, no qual mesmo um clique de aceite pode caracterizar assinatura eletrônica válida, a depender do contexto probatório.

Na União Europeia, o percurso normativo iniciou-se com a Diretiva 1999/93/CE, substituída em 2014 pelo Regulamento (UE) nº 910/2014 — conhecido pelo acrônimo eIDAS (electronic IDentification, Authentication and trust Services) —, que estabeleceu três níveis de assinatura eletrônica: simples, avançada e qualificada, sendo esta última a única equiparada, em todos os Estados-Membros, à assinatura manuscrita, por exigir certificado qualificado emitido por Prestador de Serviços de Confiança Qualificado (Qualified Trust Service Provider — QTSP) supervisionado e a criação por meio de dispositivo qualificado de criação de assinatura (UNIÃO EUROPEIA, 2014). Em 2024, o regulamento foi atualizado pelo Regulamento (UE) 2024/1183 — o chamado "eIDAS 2.0" —, que instituiu a Carteira Europeia de Identidade Digital (European Digital Identity Wallet — EUDI Wallet), a ser disponibilizada aos cidadãos europeus a partir de 2026, ampliando o escopo da identificação eletrônica transfronteiriça para além do setor público.

2.3 A trajetória brasileira: da Medida Provisória nº 2.200-2/2001 à Lei nº 14.063/2020

No Brasil, o marco fundacional da assinatura eletrônica com valor jurídico pleno é a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e criou presunção de veracidade para documentos assinados com certificado digital no âmbito dessa infraestrutura, sob gestão do Instituto Nacional de Tecnologia da Informação (ITI) e da Autoridade Certificadora Raiz (AC-Raiz) (BRASIL, 2001). Diferentemente do modelo europeu subsequente, que reconheceu múltiplos níveis de assinatura com eficácia jurídica escalonada, a norma brasileira originalmente concentrou-se em um único padrão de confiança máxima, admitindo, por interpretação doutrinária e jurisprudencial, a validade de outras formas de assinatura eletrônica fora da ICP-Brasil mediante comprovação de autoria e integridade por outros meios.

Essa lacuna regulatória foi normatizada de modo mais explícito pela Lei nº 14.063, de 23 de setembro de 2020, promulgada no contexto da aceleração digital provocada pela pandemia de covid-19, a qual disciplinou o uso de assinaturas eletrônicas em interações com entes públicos e classificou formalmente três modalidades — simples, avançada e qualificada —, aproximando o modelo brasileiro da taxonomia europeia do eIDAS (BRASIL, 2020). No plano da documentação fiscal, paralelamente, o Brasil desenvolveu, desde 2005, sob coordenação do Conselho Nacional de Política Fazendária (CONFAZ) e da Receita Federal, o modelo da Nota Fiscal Eletrônica (NF-e), disciplinado inicialmente pelo Ajuste SINIEF nº 07/2005, tornando-se referência internacional de modelo de clearance (autorização prévia da autoridade fiscal antes da emissão do documento), posteriormente replicado, com variações, por países como México, Chile, Itália e Índia.

2.4 Do documento fiscal em papel ao Continuous Transaction Control

A evolução da documentação fiscal eletrônica pode ser descrita em três gerações. A primeira geração, vigente até meados dos anos 2000, correspondia à digitalização passiva: notas fiscais permaneciam essencialmente documentos em papel, eventualmente digitalizados para arquivamento, sem qualquer intervenção estrutural da autoridade fiscal no momento da emissão. A segunda geração, iniciada com pioneiros como o Chile (2003) e consolidada pelo Brasil a partir de 2006 com a NF-e, introduziu o modelo de clearance: o documento fiscal, estruturado em formato

XML e assinado digitalmente pelo emitente, é submetido à autoridade fiscal para validação e autorização antes de sua entrega ao destinatário, criando um registro público em tempo real de cada transação tributável.

A terceira geração, em curso desde aproximadamente 2018 e ainda em expansão, caracteriza-se pela ampliação dos modelos de Continuous Transaction Control (CTC) para além da nota fiscal de venda, abrangendo relatórios periódicos digitais (Standard Audit File for Tax — SAF-T, adotado por Portugal, Romênia e Polônia), sistemas de compensação centralizada (Sistema Nazionale di Interscambio — SDI, na Itália, desde 2019; Krajowy System e-Faktur — KSeF, na Polônia), e o próprio pacote europeu ViDA, que projeta, até 2030-2035, a obrigatoriedade de e-reporting digital em tempo real para operações intracomunitárias em toda a União Europeia (INNOWISE, 2026). Esse movimento é acompanhado por iniciativas de interoperabilidade, como a rede PEPPOL (Pan-European Public Procurement OnLine), adotada não apenas na Europa, mas também em Singapura e na Austrália, como infraestrutura de troca de documentos eletrônicos estruturados entre parceiros comerciais (SAVIC TECHNOLOGIES, 2026).

2.5 Evolução das soluções SAP para documentos eletrônicos e conformidade fiscal

A resposta da SAP SE a esse cenário regulatório fragmentado evoluiu em paralelo à própria evolução dos mandatos fiscais nacionais. Em uma primeira fase, ainda sob o SAP ERP Central Component (SAP ECC), a compatibilização com exigências locais — como a NF-e brasileira — era realizada por meio de desenvolvimentos específicos por país (add-ons de localização), muitas vezes mantidos por parceiros regionais ou pela própria SAP em componentes segregados, como o histórico "SAP NF-e", com integração pontual a cada autoridade fiscal e reduzida padronização entre países.

Uma segunda fase, iniciada por volta de 2013, consolidou-se com o SAP Document Compliance (posteriormente rebatizado SAP Advanced Compliance Reporting — ACR — e, para documentos eletrônicos, eDocument Framework), que introduziu um modelo técnico comum — um framework único de criação, mapeamento e monitoramento de documentos eletrônicos — reutilizável entre países, ainda que a lógica de cada cenário local (formato XML, regras de validação,

canal de transmissão) permanecesse configurada de forma específica (COMMUNITY.SAP.COM, 2024).

A terceira e atual fase corresponde à unificação, sob a marca SAP Document and Reporting Compliance (SAP DRC), lançada oficialmente em 2020 e hoje nativa do SAP S/4HANA, integrando em uma única solução dois pilares antes tratados separadamente: (i) os documentos eletrônicos (eInvoicing), cobrindo emissão, recepção, validação e transmissão de notas fiscais e documentos de transporte eletrônicos; e (ii) os relatórios estatutários (statutory reporting), cobrindo declarações periódicas obrigatórias, como SAF-T, EC Sales Lists e apurações de IVA (FIS-GMBH, 2026). Segundo dados de mercado, a solução cobre atualmente da ordem de quinhentos cenários de conformidade em mais de cinquenta países (SAVIC TECHNOLOGIES, 2026; APPLIUM, 2026), consolidando o princípio arquitetural "standardize globally, comply locally", central para corporações que operam um único core model de S/4HANA em escala global.

3 SAP S/4HANA E A ARQUITETURA DO DOCUMENT AND REPORTING COMPLIANCE

3.1 Visão geral funcional do SAP DRC

O SAP Document and Reporting Compliance organiza-se, do ponto de vista funcional, em torno de dois domínios complementares: o domínio dos documentos eletrônicos transacionais (eDocuments) — notas fiscais eletrônicas, conhecimentos de transporte eletrônicos, notas de débito e crédito — e o domínio dos relatórios estatutários periódicos, exigidos por autoridades fiscais e regulatórias em bases mensais, trimestrais ou anuais (TJC GROUP, 2026). O fluxo típico do domínio transacional tem início na contabilização de um documento de origem no SAP S/4HANA — por exemplo, uma fatura de venda originada de uma ordem de vendas (SD) ou um lançamento contábil (FI) —, evento que dispara, de forma automática e orientada a regras, a criação de uma instância de documento eletrônico (eDocument) na tabela de controle correspondente (SAP-PRESS, 2025).

Esse eDocument é então submetido a um processo de mapeamento estrutural, no qual os dados oriundos do documento de origem são transformados no formato

exigido pela autoridade fiscal ou pela rede de intercâmbio de destino — por exemplo, o esquema XML da NF-e brasileira, o esquema FatturaPA italiano, ou o formato UBL utilizado pela rede PEPPOL. Após validação sintática e semântica, o documento é assinado digitalmente, quando exigido, e transmitido ao destinatário — autoridade fiscal, plataforma governamental ou parceiro de negócios — por meio de canal seguro. Durante todo o ciclo, o SAP DRC mantém trilhas de auditoria e rastreamento de status (criado, enviado, aceito, rejeitado, cancelado), essenciais tanto para a operação corrente quanto para fins de comprovação em fiscalizações (SAP-PRESS, 2025).

3.2 eDocument Framework

O eDocument Framework constitui o núcleo técnico do domínio transacional do SAP DRC. Tecnicamente, compõe-se de estruturas de dados genéricas (independentes de país), responsáveis por armazenar o estado e o conteúdo de cada documento eletrônico, e de camadas de customização específicas por localização (country-specific logic), implementadas mediante Business Add-Ins (BAdIs) e classes de mapeamento que traduzem o modelo de dados genérico para o esquema exigido por cada jurisdição. Essa separação entre núcleo genérico e camada de localização é o que permite à SAP incorporar novos países ou novos cenários regulatórios sem alterar a lógica central do framework, apenas adicionando ou atualizando os componentes de mapeamento correspondentes (COMMUNITY.SAP.COM, 2024).

3.3 Application Interface Framework (AIF)

A transmissão e o monitoramento de interfaces do eDocument Framework apoiam-se, em grande parte dos cenários, no SAP Application Interface Framework (AIF), componente responsável por padronizar o tratamento de erros, o mapeamento de campos, o mapeamento de valores (value mapping) e a reprocessabilidade de mensagens com falha. Do ponto de vista de integração de assinatura eletrônica, o AIF desempenha papel relevante como camada de orquestração: é nele que falhas na etapa de assinatura digital — por exemplo, indisponibilidade do provedor de confiança, certificado expirado, ou rejeição por parte da autoridade fiscal — podem ser monitoradas, reprocessadas e escaladas por meio de alertas operacionais, sem

necessidade de intervenção direta no código-fonte do processo (COMMUNITY.SAP.COM, 2024).

3.4 Compliance Cockpit, SAP Cloud Connector e integração com autoridades fiscais

O Compliance Cockpit constitui a interface operacional do SAP DRC, implementada diretamente no sistema S/4HANA e destinada à revisão, correção e liberação de documentos eletrônicos antes de sua transmissão, bem como ao acompanhamento consolidado do status de cada obrigação fiscal, por país e por tipo de documento (VALANTIC, 2025). Para a comunicação efetiva com autoridades fiscais, plataformas governamentais e redes de intercâmbio, o SAP DRC integra-se, na maior parte dos cenários mais recentes, ao SAP Business Technology Platform (SAP BTP) — em particular ao serviço SAP Cloud Integration e ao SAP Cloud Connector —, responsáveis por estabelecer o canal seguro de comunicação, tipicamente por meio de conexão criptografada (Transport Layer Security — TLS), autenticação mútua por certificado e, quando exigido, assinatura digital do payload transmitido (VALANTIC, 2025).

Esse desenho arquitetural — sistema transacional on-premise ou em nuvem privada (S/4HANA), camada de integração em nuvem pública (SAP BTP) e destino externo (autoridade fiscal ou rede de parceiros) — reflete uma tendência mais ampla da arquitetura SAP contemporânea, na qual funções de integração, antes residentes dentro do próprio ERP, migram progressivamente para camadas de middleware em nuvem, favorecendo atualização mais ágil frente a mudanças regulatórias frequentes, sem exigir upgrade do núcleo transacional.

3.5 Statutory Reporting e o modelo declaratório periódico

Complementarmente ao fluxo transacional, o pilar de Statutory Reporting do SAP DRC organiza a extração, a consolidação e a formatação de relatórios fiscais periódicos — como apurações de Imposto sobre o Valor Agregado (IVA/VAT), Standard Audit Files (SAF-T) e listas recapitulativas de operações intracomunitárias (EC Sales Lists) —, com trilha de aprovação interna e submissão ao portal da autoridade competente. Esse pilar compartilha com o domínio transacional a mesma

lógica arquitetural de separação entre núcleo genérico e conteúdo legal específico por país, permitindo reaproveitamento de componentes de extração de dados entre diferentes obrigações declaratórias de uma mesma jurisdição (SNI TECHNOLOGY, 2026).

4 INTEGRAÇÃO DE ASSINATURA ELETRÔNICA EM AMBIENTES SAP S/4HANA GLOBAIS

4.1 Modelos de assinatura eletrônica e sua correspondência normativa

A integração técnica de assinatura eletrônica ao SAP DRC não pode ser dissociada da classificação jurídica exigida em cada jurisdição. De modo geral, três níveis de assinatura eletrônica — simples, avançada e qualificada — encontram correspondência, com nomenclaturas variáveis, tanto no Regulamento eIDAS europeu quanto na Lei nº 14.063/2020 brasileira. A assinatura eletrônica simples corresponde a mecanismos de identificação de baixa robustez probatória (por exemplo, login e senha), raramente suficientes, isoladamente, para documentos fiscais de maior criticidade. A assinatura eletrônica avançada exige vinculação inequívoca ao signatário e capacidade de detecção de alterações posteriores ao documento, sem necessariamente depender de certificado emitido por autoridade certificadora credenciada. A assinatura eletrônica qualificada, por sua vez, exige certificado digital qualificado — no Brasil, emitido no âmbito da ICP-Brasil; na União Europeia, por Prestador de Serviços de Confiança Qualificado — e é a única modalidade dotada de presunção legal de autenticidade equivalente à assinatura manuscrita em todas as jurisdições que adotam esse modelo.

No contexto do SAP DRC, a exigência normativa de cada país determina o nível de assinatura tecnicamente implementado em cada cenário de eDocument. Para a NF-e brasileira, por exemplo, exige-se assinatura digital com certificado ICP-Brasil do tipo A1 ou A3, aplicada sobre o XML do documento antes de sua transmissão à Secretaria da Fazenda estadual competente; para a FatturaPA italiana, admite-se tanto a assinatura digital qualificada quanto, em determinados fluxos via Sistema di Interscambio (SDI), a autenticação do canal de transmissão como mecanismo substitutivo; para cenários PEPPOL, a confiança é estabelecida primariamente pela

rede de pontos de acesso certificados (Access Points), com uso de assinatura digital sobre o envelope de transporte.

4.2 Padrões técnicos de assinatura digital de documentos: XAdES, PAdES e CAdES

Do ponto de vista técnico-criptográfico, a integração de assinatura eletrônica a documentos fiscais eletrônicos apoia-se, majoritariamente, em três famílias de padrões desenvolvidos pelo European Telecommunications Standards Institute (ETSI), coletivamente conhecidas como AdES (Advanced Electronic Signatures): XAdES (XML Advanced Electronic Signatures — ETSI EN 319 132), aplicável a documentos estruturados em XML, formato predominante na quase totalidade dos esquemas de nota fiscal eletrônica, incluindo a NF-e brasileira; PAdES (PDF Advanced Electronic Signatures — ETSI EN 319 142), aplicável a documentos em formato PDF, com base na especificação ISO 32000-2, relevante para relatórios estatutários e documentos contratuais anexos a processos fiscais; e CAdES (CMS Advanced Electronic Signatures — ETSI EN 319 122), baseado na sintaxe CMS (Cryptographic Message Syntax) da IETF, utilizado sobretudo quando o documento assinado não deve ser alterado em sua estrutura binária original.

Cada uma dessas famílias admite diferentes níveis de robustez — do nível básico (B-B), que garante apenas a assinatura em si, até níveis com carimbo de tempo (B-T), com dados de validação incorporados (B-LT) e com arquivamento de longo prazo (B-LTA) —, sendo a escolha do nível determinada por exigências regulatórias específicas de retenção documental, tipicamente entre cinco e dez anos, a depender da jurisdição fiscal. No ecossistema SAP DRC, essa assinatura pode ser aplicada em dois pontos distintos do fluxo: (i) internamente, mediante bibliotecas criptográficas embarcadas no próprio S/4HANA ou no SAP BTP; ou (ii) externamente, mediante integração com um Provedor de Serviços de Confiança (Trust Service Provider — TSP) terceirizado, acessado via API.

4.3 Arquitetura de integração com Provedores de Serviços de Confiança (TSP)

A arquitetura de referência para integração de assinatura eletrônica qualificada ao SAP DRC em cenários globais tipicamente segue um padrão de três camadas. Na primeira camada, o S/4HANA gera o documento eletrônico não

assinado (payload), a partir do eDocument Framework, contendo todos os dados fiscalmente relevantes já validados estrutural e semanticamente. Na segunda camada, o SAP BTP — por meio de SAP Cloud Integration (Integration Suite) ou de desenvolvimento customizado sobre Cloud Foundry — orquestra a chamada ao serviço externo de assinatura, tipicamente exposto como API REST ou SOAP pelo Prestador de Serviços de Confiança, transmitindo o payload por canal TLS mutuamente autenticado e recebendo, em resposta, o documento assinado (com assinatura embarcada, no padrão enveloped, ou destacada, no padrão detached, conforme o esquema exigido). Na terceira camada, o documento assinado retorna ao eDocument Framework para transmissão final à autoridade fiscal ou à rede de parceiros, com o respectivo registro de trilha de auditoria.

Esse modelo de integração via API é preferido, em ambientes corporativos globais, ao uso de hardware security modules (HSM) fisicamente instalados em cada país de operação, pela maior flexibilidade operacional e pela possibilidade de centralizar contratos com um número reduzido de TSPs de abrangência multijurisdicional — embora, em determinados países, a legislação local exija que a chave privada de assinatura permaneça sob custódia exclusiva do próprio contribuinte, ou de autoridade certificadora nacional, restringindo o uso de provedores estrangeiros de assinatura como serviço (Signature as a Service — SaaS de assinatura).

4.4 Gestão de certificados digitais e ciclo de vida em ambiente multipaís

Um desafio operacional recorrente em implementações SAP DRC de escopo global é a gestão do ciclo de vida de certificados digitais — emissão, renovação, revogação e substituição — distribuídos entre dezenas de entidades legais (company codes), cada qual potencialmente sujeita a autoridade certificadora distinta, prazo de validade distinto (certificados ICP-Brasil do tipo A1, por exemplo, têm validade de até um ano, ao passo que certificados A3 chegam a três anos) e procedimento de renovação distinto. A ausência de gestão centralizada e automatizada desse ciclo de vida é apontada, na literatura técnica de implementação, como uma das causas mais frequentes de interrupção não planejada em processos de emissão de documentos

fiscais eletrônicos, sobretudo quando certificados expiram sem substituição tempestiva (SAVIC TECHNOLOGIES, 2026).

Como resposta a esse risco, arquiteturas maduras de integração incorporam mecanismos de monitoramento proativo de expiração de certificados — tipicamente implementados na camada de integração do SAP BTP ou em ferramentas de gestão de certificados de terceiros —, com alertas automáticos disparados entre trinta e sessenta dias antes do vencimento, e processos de troca de certificado (certificate rollover) desenhados para não interromper o fluxo de emissão em produção.

4.5 Panorama comparativo por região

A comparação entre regiões evidencia significativa heterogeneidade na integração entre assinatura eletrônica e conformidade fiscal digital. No Brasil, o modelo de clearance da NF-e exige assinatura digital ICP-Brasil aplicada pelo próprio emitente antes do envio à Secretaria da Fazenda, com validação e autorização em tempo real; a integração no SAP DRC, portanto, concentra-se na camada de geração e assinatura local, com uso frequente de certificados A1 armazenados de forma segura no próprio ambiente corporativo ou em cofres de chaves (key vaults) na nuvem. Na União Europeia, a heterogeneidade entre os Estados-Membros é ainda maior: países como a Itália adotam modelo de clearance centralizado via SDI, com validação e retransmissão pela própria autoridade fiscal; países como a Alemanha, com a introdução da XRechnung e do ZUGFeRD a partir de 2025, adotam inicialmente modelo de recepção obrigatória sem clearance centralizada, com plena obrigatoriedade de emissão prevista para 2027-2028 (MUNICH-ENTERPRISE, 2025).

Na Índia, o modelo de e-invoicing exige geração de um Invoice Reference Number (IRN) pelo Invoice Registration Portal (IRP) governamental antes da emissão válida da fatura, com assinatura digital aplicada pela própria autoridade sobre o documento retornado ao contribuinte — inversão, portanto, do modelo brasileiro, em que a assinatura é aposta pelo emitente. Na Polônia, a introdução do sistema centralizado KSeF (Krajowy System e-Faktur) segue cronograma de obrigatoriedade escalonada até 2026-2027, exigindo autenticação e, em determinados cenários, assinatura qualificada para acesso ao portal (SAP COMMUNITY, 2026).

Esse mosaico regulatório é precisamente o que justifica, do ponto de vista de arquitetura corporativa, a adoção de uma camada de integração desacoplada e configurável — como o eDocument Framework do SAP DRC —, capaz de absorver modelos de assinatura tão distintos sem exigir reformulação do núcleo transacional do S/4HANA a cada nova exigência nacional.

5 ANÁLISE CRÍTICA: DESAFIOS, RISCOS E TENDÊNCIAS

5.1 Desafios técnicos de integração

Do ponto de vista técnico, a integração de assinatura eletrônica ao SAP DRC em ambientes globais enfrenta ao menos quatro classes recorrentes de desafio. A primeira refere-se à heterogeneidade de formatos e protocolos exigidos por diferentes autoridades fiscais, que obriga times de integração a manter múltiplos conectores, versões de esquema XML e regras de validação simultaneamente ativos, com custo de manutenção crescente à medida que a operação corporativa se expande para novos países. A segunda diz respeito à latência e à disponibilidade dos serviços governamentais de validação, cuja indisponibilidade — situação recorrente em picos de fechamento fiscal — pode bloquear o fluxo de faturamento caso a arquitetura não preveja mecanismos robustos de reprocessamento assíncrono e fila de contingência.

A terceira classe de desafio relaciona-se à governança de chaves criptográficas em ambientes de nuvem híbrida, na qual a chave privada de assinatura pode residir em diferentes camadas — dentro do próprio S/4HANA, em um cofre de segredos do SAP BTP, ou sob custódia de um Provedor de Serviços de Confiança externo —, exigindo controles de acesso, segregação de funções e trilhas de auditoria consistentes entre ambientes de diferentes provedores de nuvem. A quarta classe refere-se ao versionamento regulatório: mudanças frequentes em esquemas XML, em regras de validação e em endpoints governamentais — como as sucessivas atualizações do layout da NF-e brasileira ou as fases de implementação do ViDA europeu — exigem processo de gestão de mudanças (change management) capaz de testar e homologar alterações sem interromper a operação corrente.

5.2 Desafios jurídicos e regulatórios

No plano jurídico, a operação de um único ambiente S/4HANA global impõe às corporações multinacionais o desafio de assegurar, simultaneamente, o cumprimento de exigências potencialmente conflitantes entre jurisdições — por exemplo, requisitos de residência de dados (data residency) que determinam que certos documentos fiscais, ou as chaves utilizadas para assiná-los, permaneçam fisicamente armazenados dentro do território nacional, em contraposição à lógica de centralização típica de arquiteturas de nuvem pública multirregionais. Some-se a isso a diversidade de prazos de retenção documental obrigatória — que variam, a depender do país, entre cinco e vinte anos —, exigindo estratégias de arquivamento de longo prazo (frequentemente amparadas em assinaturas no nível B-LTA dos padrões AdES) compatíveis com a obsolescência tecnológica dos próprios algoritmos criptográficos utilizados na assinatura original.

Adicionalmente, a validade jurídica extraterritorial de uma assinatura eletrônica qualificada nem sempre é automática: um certificado emitido no âmbito da ICP-Brasil não é automaticamente reconhecido como qualificado no âmbito do eIDAS europeu, e vice-versa, exigindo, em determinados cenários de comércio internacional, soluções de reconhecimento mútuo, apostilamento eletrônico ou dupla assinatura, o que amplia a complexidade jurídica da integração técnica correspondente.

5.3 Segurança da informação e criptografia pós-quântica

Sob a ótica de segurança da informação, a concentração, em uma única plataforma de integração — como o SAP BTP —, do fluxo de assinatura de documentos fiscais de múltiplas entidades legais e países eleva a criticidade dessa camada como potencial ponto único de falha (single point of failure) e como alvo de ataques direcionados, justificando a adoção de práticas de segurança reforçadas: autenticação multifator para acesso administrativo, segregação de ambientes por criticidade, monitoramento contínuo de anomalias (Security Information and Event Management — SIEM) e testes periódicos de penetração sobre os endpoints de integração expostos a provedores externos de assinatura.

Em horizonte de médio prazo, a maturação de computadores quânticos com capacidade suficiente para comprometer algoritmos de criptografia assimétrica

atualmente empregados — como RSA e curvas elípticas (ECDSA), ambos amplamente utilizados nos padrões XAdES, PAdES e CAdES — motivou o Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) a padronizar, em 2024, os primeiros algoritmos de criptografia pós-quântica (post-quantum cryptography), como o CRYSTALS-Dilithium (padronizado como FIPS 204). A transição desses novos algoritmos para os padrões de assinatura de documentos fiscais eletrônicos ainda não foi formalmente endereçada pela maioria das autoridades tributárias globais, configurando-se como área de atenção prospectiva relevante para arquitetos de integração em ambientes SAP de longo prazo, dado o extenso período de retenção documental exigido pela legislação fiscal.

5.4 Tendências: ViDA, EUDI Wallet e inteligência artificial aplicada à conformidade

Três tendências relevantes despontam para a evolução da integração entre assinatura eletrônica e conformidade fiscal em ambientes S/4HANA nos próximos anos. Primeiramente, a implementação progressiva do pacote europeu ViDA deverá ampliar, a partir de 2028-2030, a exigência de e-reporting digital em tempo real para transações intracomunitárias, com potencial padronização em torno do formato UBL/PEPPOL, o que poderá reduzir — ainda que não eliminar — a fragmentação atualmente observada entre países europeus (INNOWISE, 2026).

Em segundo lugar, a disseminação da Carteira Europeia de Identidade Digital (EUDI Wallet), a partir da entrada em vigor do eIDAS 2.0, poderá alterar o modelo de emissão e verificação de assinaturas eletrônicas qualificadas, ao permitir que cidadãos e representantes legais de pessoas jurídicas apliquem assinaturas qualificadas diretamente a partir de dispositivos móveis, com potencial impacto na forma como sistemas ERP, incluindo o SAP S/4HANA, integram-se a mecanismos de assinatura centrados no usuário (user-centric signing), em contraposição ao modelo predominantemente automatizado e desatendido (unattended signing) hoje utilizado na maioria dos cenários de faturamento eletrônico em massa.

Em terceiro lugar, observa-se crescente incorporação de técnicas de inteligência artificial e aprendizado de máquina em módulos de conformidade fiscal — inclusive no próprio SAP DRC e em soluções complementares do portfólio SAP

Business AI —, voltadas à detecção antecipada de inconsistências em documentos fiscais antes de sua submissão, à predição de rejeições por autoridades fiscais com base em padrões históricos, e à automação de reconciliação entre documentos emitidos e obrigações declaratórias periódicas, tendência que deverá se intensificar à medida que o volume de documentos eletrônicos processados globalmente continue a crescer.

6 METODOLOGIA

O presente estudo caracteriza-se, quanto à natureza, como pesquisa qualitativa; quanto aos objetivos, como pesquisa exploratória e descritiva; e quanto aos procedimentos técnicos, como pesquisa bibliográfica e documental, nos termos da classificação metodológica consolidada por Gil (2019). A pesquisa bibliográfica apoiou-se em literatura especializada em direito digital, direito tributário eletrônico e arquitetura de sistemas ERP, ao passo que a pesquisa documental incidiu sobre fontes primárias de natureza normativa — textos legais nacionais e estrangeiros, regulamentos da União Europeia, normas técnicas do ETSI e da ISO — e sobre documentação técnica oficial publicada pela SAP SE relativa ao SAP Document and Reporting Compliance e ao eDocument Framework.

A seleção das fontes obedeceu a critérios de relevância temática, atualidade — priorizando-se, sempre que disponível, a versão normativa ou documental mais recente em vigor — e autoridade da fonte, com preferência por textos legais originais, documentação oficial do fabricante e material técnico publicado por consultorias especializadas certificadas em implementação SAP. A análise foi conduzida em perspectiva histórico-comparativa, correlacionando marcos temporais da evolução regulatória da assinatura eletrônica com marcos temporais da evolução arquitetural das soluções SAP de conformidade fiscal, de modo a evidenciar padrões de causalidade e antecipação mútua entre regulação e tecnologia. Reconhece-se, como limitação metodológica, o caráter dinâmico do objeto de estudo: por tratar-se de tema sujeito a atualização normativa e tecnológica constante, os dados e cenários regulatórios aqui descritos refletem o estado da arte disponível até a data de elaboração deste artigo, podendo sofrer alterações supervenientes.

7 CONSIDERAÇÕES FINAIS

A reconstituição histórica empreendida neste artigo evidencia que a integração entre assinatura eletrônica e conformidade fiscal digital em ambientes SAP S/4HANA globais não constitui fenômeno isolado, mas resultado de trajetórias regulatórias e tecnológicas que se desenvolveram, ao longo de aproximadamente três décadas, em relação de mútua influência: avanços na criptografia de chave pública e no reconhecimento jurídico da assinatura eletrônica viabilizaram a digitalização de obrigações fiscais acessórias, ao passo que a crescente sofisticação dos modelos de controle contínuo de transações por parte das administrações tributárias pressionou, por sua vez, a evolução das arquiteturas de ERP em direção a soluções cada vez mais modulares, orientadas a APIs e desacopladas do núcleo transacional.

A análise da arquitetura do SAP DRC revela que essa modularidade — expressa na separação entre um eDocument Framework genérico e camadas de localização específicas por país, e na migração progressiva de funções de integração para o SAP Business Technology Platform — constitui resposta arquitetural direta à fragmentação regulatória internacional, permitindo que corporações multinacionais mantenham um único core model global de S/4HANA sem abrir mão da conformidade com exigências criptográficas, documentais e procedimentais tão heterogêneas quanto as observadas entre Brasil, União Europeia, Índia e Polônia.

Como principais desafios identificados, destacam-se a gestão do ciclo de vida de certificados digitais em escala multinacional, a governança de chaves criptográficas em ambientes de nuvem híbrida, a compatibilização entre exigências conflitantes de residência de dados e centralização arquitetural, e a necessidade de acompanhamento contínuo de mudanças regulatórias frequentes. Como tendências relevantes para o horizonte próximo, aponta-se a expansão dos modelos de e-reporting em tempo real no âmbito do pacote europeu ViDA, a disseminação de mecanismos de assinatura centrados no usuário viabilizados pela Carteira Europeia de Identidade Digital, e a incorporação crescente de inteligência artificial em processos de validação e reconciliação fiscal.

Conclui-se que a maturidade da integração entre assinatura eletrônica e SAP DRC em S/4HANA não deve ser avaliada apenas por critérios de conformidade pontual com a legislação vigente em cada país, mas, sobretudo, pela capacidade da

arquitetura corporativa de absorver, de forma ágil e governada, mudanças regulatórias futuras — capacidade que, à luz da trajetória histórica reconstituída neste estudo, tende a ser tanto mais robusta quanto maior for o grau de desacoplamento entre o núcleo transacional do ERP e as camadas de integração, assinatura e conformidade fiscal. Como agenda de pesquisa futura, sugere-se o aprofundamento empírico, por meio de estudos de caso multissetoriais, do impacto quantitativo de falhas de integração de assinatura eletrônica sobre indicadores de continuidade de negócio (order-to-cash), bem como a investigação sistemática dos impactos da criptografia pós-quântica sobre a validade jurídica de longo prazo de documentos fiscais eletrônicos já assinados.

REFERÊNCIAS

- APPLIUM. SAP Document and Reporting Compliance (DRC). 2026. Disponível em: https://www.applium.com/en/solutions/sap-document-and-reporting-compliance/. Acesso em: 1 ago. 2026.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14724: informação e documentação — trabalhos acadêmicos — apresentação. Rio de Janeiro: ABNT, 2011.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: informação e documentação — referências — elaboração. Rio de Janeiro: ABNT, 2018.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520: informação e documentação — citações em documentos — apresentação. Rio de Janeiro: ABNT, 2023.
- BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil. Diário Oficial da União, Brasília, DF, 2001.
- BRASIL. Lei nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos. Diário Oficial da União, Brasília, DF, 2020.
- CONSELHO NACIONAL DE POLÍTICA FAZENDÁRIA. Ajuste SINIEF nº 07, de 30 de setembro de 2005. Institui a Nota Fiscal Eletrônica e o Documento Auxiliar da Nota Fiscal Eletrônica. Brasília: CONFAZ, 2005.
- DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. IEEE Transactions on Information Theory, v. 22, n. 6, p. 644-654, 1976.
- FIS-GMBH. SAP DRC — SAP Document and Reporting Compliance. 2026. Disponível em: https://www.fis-gmbh.de/en/sap-wiki/sap-drc/. Acesso em: 3 ago. 2026.
- GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2019.

- INNOWISE. SAP e-invoicing: document and reporting compliance. 2026. Disponível em: https://innowise.com/blog/sap-drc-e-invoicing/. Acesso em: 5 ago. 2026.
- MUNICH ENTERPRISE. E-invoicing with SAP DRC and eDocument — SAP Document and Reporting Compliance. 2025. Disponível em: https://www.munich-enterprise.com/. Acesso em: 7 ago. 2026.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. FIPS 204: Module-Lattice-Based Digital Signature Standard. Gaithersburg: NIST, 2024.
- PINHEIRO, Patrícia Peck. Direito digital. 7. ed. São Paulo: Saraiva Educação, 2021.
- RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, v. 21, n. 2, p. 120-126, 1978.
- SAP COMMUNITY. SAP Document and Reporting Compliance. 2026. Disponível em: https://pages.community.sap.com/topics/document-reporting-compliance. Acesso em: 9 ago. 2026.
- SAP SE. eInvoice with SAP DRC: electronic document processing using extensibility features. SAP Community, 2024. Disponível em: https://community.sap.com/. Acesso em: 11 ago. 2026.
- SAP-PRESS. What is SAP Document and Reporting Compliance (SAP DRC)? 2025. Disponível em: https://blog.sap-press.com/what-is-sap-document-and-reporting-compliance-sap-drc. Acesso em: 13 ago. 2026.
- SAVIC TECHNOLOGIES. SAP DRC: document and reporting compliance — enterprise implementation guide. 2026. Disponível em: https://www.savictech.com/insights/. Acesso em: 15 ago. 2026.
- SNI TECHNOLOGY. SAP DRC solution — document & reporting compliance. 2026. Disponível em: https://snitechnology.net/sap-document-reporting-compliance/. Acesso em: 17 ago. 2026.
- TJC GROUP. What is SAP Document and Reporting Compliance A guide to SAP DRC. 2026. Disponível em: https://www.tjc-group.com/blogs/what-is-sap-document-and-reporting-compliance-a-guide-to-sap-drc/. Acesso em: 20 ago. 2026.
- UNCITRAL. Model Law on Electronic Signatures with Guide to Enactment. Viena: United Nations, 2001.
- UNIÃO EUROPEIA. Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 (eIDAS). Jornal Oficial da União Europeia, 2014.
- UNIÃO EUROPEIA. Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024. Jornal Oficial da União Europeia, 2024.
- UNITED STATES CONGRESS. Electronic Signatures in Global and National Commerce Act (ESIGN Act). Public Law 106-229, 2000.
- VALANTIC. SAP DRC: implementing e-invoices securely and efficiently. 2025. Disponível em: https://www.valantic.com/en/blog/convert-e-invoices-with-sap-drc/. Acesso em: 22 ago. 2026.