Manual de Segurança

Split Payment

Reforma Tributária

Manual de Segurança

Versão 1.0.0 | Setembro de 2026

SUMÁRIO

CAPÍTULO 1 – DISPOSIÇÕES INICIAIS

1.1 INTRODUÇÃO

Este Manual de Segurança estabelece os requisitos técnicos e operacionais mínimos para proteger a comunicação, o processamento, o armazenamento e a auditoria dos dados do Split Payment dos tributos CBS e IBS. Ele orienta os Prestadores de Serviços de Pagamento (PSPs), a Núclea e a Plataforma Pública quanto aos controles de autenticação, autorização, criptografia, assinatura, integridade, monitoração, evidências e resposta a incidentes.

Por ser um ecossistema multi-institucional e regulado, a segurança do Split Payment não se restringe à proteção da API. Ela abrange também a identidade institucional dos participantes, a integridade dos informes, o consumo do Retorno Super Inteligente, o envio do Informe de Segregação, além da rastreabilidade de ponta a ponta, que inclui a capacidade de demonstrar o cumprimento dos ANS e das responsabilidades de cada parte.

As diretrizes aqui definidas incorporam requisitos de confidencialidade, integridade, autenticidade, não repúdio, sigilo fiscal, proteção de dados e rastreabilidade, dada a natureza sensível dos dados financeiros, fiscais e operacionais tratados. Como referência de governança, os controles permanecem compatíveis com a LGPD, com as normas e orientações aplicáveis do Banco Central do Brasil, com boas práticas de segurança cibernética e com os referenciais ISO/IEC 27001 e ISO/IEC 27002, sem prejuízo de requisitos mais específicos definidos nos demais manuais e no Regulamento.

Este manual integra um conjunto de documentos do Split Payment, cada um com finalidade específica, conforme a tabela a seguir.

Documento	Finalidade
Manual de Operações	Funcionamento operacional, fluxos, regras de cálculo, experiência do usuário
Manual de Integração + Documento OpenAPI	Especificação técnica da API, contratos de mensagens, endpoints, dicionário de campos
Manual de Tempos	Prazos, janelas operacionais, ANS e marcos temporais
Manual de Redes	Arquitetura de conexão, topologia, capacidade e resiliência
Manual de Segurança	Autenticação, criptografia, auditoria e controles de proteção
Manual de Habilitação de Participantes	Checklist de conformidade para entrada de novos PSPs no Split Payment, playbooks de habilitação e desabilitação, governança de incidentes
Plano de Implantação	Cronograma de implantação, marcos, prazos de envio dos formulários e penalidades por etapa

O conteúdo deste manual é complementar aos demais. Quando um tema é tratado em outro documento, este manual não reproduz o detalhamento técnico que pertence ao manual correspondente.

Nota: definições pendentes ao longo do documento estão marcadas em amarelo, e serão atualizadas em uma nova versão deste documento.

1.2 ESCOPO

Este manual aplica-se à **Fase 1 - B2B Opcional do Split Payment** e contempla os arranjos Boleto, Pix Dinâmico, Pix Automático, Pix Estático, TED e TEF (Book Transfer). Abrange os controles de segurança das integrações entre os participantes e a Plataforma Pública, bem como os controles internos necessários para preservar a integridade, a confidencialidade, a disponibilidade, a rastreabilidade e o não repúdio das mensagens e dos valores processados. Esses controles estão organizados nas seguintes categorias:

- **Autenticação e autorização:** autenticação mTLS, gestão de certificados e autorização por participante, arranjo e endpoint.
- **Assinatura e integridade:** assinatura JWS/JWT, distribuição de chaves via JWKS e integridade de payload.
- **Registro, observabilidade e resposta:** logs, auditoria, evidências, monitoração, alertas e tratamento de incidentes, incluindo a segurança de terceiros que operem por delegação.

Não fazem parte do escopo deste manual o processo de habilitação de participantes, os casos de teste de homologação, os formulários de cadastro e o canal de solicitação de logs à Plataforma Pública, todos tratados no Manual de Habilitação de Participantes. Os contratos de mensagens, o dicionário de campos e as regras de negócio do Split Payment são tratados no Manual de Integração e na documentação OpenAPI.

1.3 PÚBLICO-ALVO

Destina-se a arquitetos de segurança, equipes de segurança da informação, responsáveis por PKI, times de integração e de API, equipes de redes, SRE, NOC, SOC, auditoria, compliance e responsáveis técnicos dos PSPs e da Núclea, incluindo os PSPs que atuem por delegação em nome de outro participante.

CAPÍTULO 2 – MODELO DE CONFIANÇA

Este capítulo define quem são os atores do Split Payment e as fronteiras de confiança entre eles, além da separação entre os ambientes de homologação e de produção.

2.1 ATORES E FRONTEIRAS DE CONFIANÇA

O modelo de confiança parte da premissa de que cada participante é responsável pela sua própria identidade técnica, pelas informações que envia e pelas delegações que concede. A Plataforma Pública atua como hub de comunicação e validação, mas não substitui os controles internos de cada PSP ou da Núclea.

Quando um PSP opera em nome de outro participante, por exemplo prestando o serviço de conexão à Plataforma Pública, ele permanece sendo um PSP e continua sujeito aos mesmos controles deste manual, atuando estritamente dentro do escopo que lhe foi delegado. A responsabilidade regulatória perante a Plataforma Pública permanece com o **PSP Recebedor Direto**. No arranjo Boleto, essa responsabilidade permanece com a **Núclea**.

Internamente, cada participante deve manter a segregação de funções entre a operação de integração, a gestão de chaves e certificados, a auditoria e a administração dos ambientes de produção, de modo que nenhuma pessoa ou equipe acumule o controle sobre as credenciais e sobre as evidências de seu uso.

CAPÍTULO 3 – CLASSIFICAÇÃO DE ATIVOS

Os ativos de segurança do Split Payment são classificados por nível de criticidade, o que orienta o rigor dos controles aplicáveis a cada um. Este capítulo define os níveis de classificação e as suas implicações (Seção 3.1) e apresenta o inventário dos ativos com os controles mínimos correspondentes (Seção 3.2).

3.1 NÍVEIS DE CLASSIFICAÇÃO E SUAS IMPLICAÇÕES

São adotados dois níveis para os ativos tratados neste manual. O nível determina, de forma crescente, as exigências de proteção, monitoração e resposta:

- **Alto:** ativo cujo comprometimento pode expor dados sensíveis ou fluxos operacionais. Exige proteção do material em trânsito, escopo de uso restrito, ausência de registro em claro e expiração curta, quando aplicável.
- **Crítico:** ativo cujo comprometimento permite usurpação de identidade institucional, adulteração de mensagens ou acesso indevido a dados de outro participante. Exige armazenamento seguro com acesso restrito, proteção preferencial em hardware criptográfico (HSM ou KMS), inventário e monitoração de validade, revogação emergencial e tratamento como incidente crítico.

3.2 INVENTÁRIO DE ATIVOS E CONTROLES MÍNIMOS

A tabela a seguir relaciona cada ativo ao seu nível de classificação e ao controle mínimo correspondente.

Ativo	Classificação	Controle mínimo
Certificado mTLS cliente	Crítico	Armazenamento seguro, inventário, validade monitorada e revogação emergencial.
Chave privada mTLS	Crítico	Proteção adequada das chaves privadas, com acesso restrito e exportação evitada; o uso de recursos como HSM ou KMS é recomendado quando aplicável.
Chave privada JWS	Crítico	As chaves utilizadas para assinatura devem ser armazenadas e gerenciadas de forma segura, contemplando processos de renovação e mecanismos de auditoria.
Token de stream	Alto	Não registrar em claro, escopo por PSP/arranjo e expiração curta.
Dados das transações	Alto	Trânsito protegido pelo canal mTLS sobre rede segura.

CAPÍTULO 4 – AUTENTICAÇÃO, IDENTIDADE E AUTORIZAÇÃO

Toda chamada à API da Plataforma Pública é autenticada por mTLS, tem a sua identidade vinculada ao participante e é autorizada por arranjo e por endpoint.

4.1 CADEIA DE CONFIANÇA

A validação do certificado ocorre antes do processamento HTTP. Certificados ausentes, expirados, revogados, emitidos por cadeia não confiável ou incompatíveis com o ambiente resultam em **rejeição da autenticação, sem que a requisição seja processada**.

Elemento	Requisito
Versão mínima TLS	TLS 1.2 ou superior.
Suítes permitidas	TLS 1.3: TLS_AES_128_GCM_SHA256 e TLS_CHACHA20_POLY1305_SHA256; TLS 1.2: ECDHE-RSA-AES-128-GCM-SHA256 e ECDHE-ECDSA-AES-128-GCM-SHA256. Troca de chaves ECDHE obrigatória em ambos.
Validade do certificado cliente	O certificado deve estar dentro do período de validade definido pela Autoridade Certificadora da ICP-Brasil e não pode estar expirado. Recomenda-se que o participante realize sua renovação antes do vencimento para evitar indisponibilidade operacional.
Revogação	OCSP ou CRL obrigatório. Na indisponibilidade desses serviços, sugere-se adotar comportamento fail-closed para novos handshakes ou validações, impedindo a continuidade quando o status de revogação não puder ser confirmado após o esgotamento das tentativas dentro do timeout configurado. A ocorrência deve gerar registro de evidência e alerta operacional. Para conexões já estabelecidas, poderá ser aplicada tolerância temporária controlada, em modelo fail-open, limitada a uma janela curta, devidamente monitorada e auditável. A política definitiva deverá estabelecer os critérios, limites e condições para aplicação dos comportamentos fail-open e fail-closed.
Chave privada	RSA de no mínimo 2048 bits ou ECDSA (curvas P-256/P-384), gerada e protegida com acesso restrito; recomenda-se proteção em hardware criptográfico para produção, quando aplicável.
Resolução de nomes (DNS)	Os clientes HTTP dos participantes devem sempre respeitar o TTL (Time To Live) dos servidores DNS; o descumprimento pode causar falhas de resolução de nome e indisponibilidade de acesso às APIs.

4.2 IDENTIDADE INSTITUCIONAL

A identidade técnica autenticada pelo certificado é vinculada aos identificadores de negócio e de autorização. O participante não pode declarar, por header, path ou body, um cnpjRaizPspRecDir ou um arranjo que não esteja associado ao certificado apresentado.

Vínculo obrigatório	Regra
Certificado - participante	Certificado deve identificar univocamente PSP, Núclea ou Prestador de Serviço de Conexão autorizado.
cnpjRaizPspRecDir	cnpjRaizPspRecDir usado em endpoints específicos deve pertencer ao participante.
Participante - arranjo/endpoint	Acesso deve ser negado para arranjos não homologados ou não delegados.

4.3 AUTORIZAÇÃO POR ARRANJO E ENDPOINT

O controle de acesso por endpoint é aplicado na camada de gateway e de roteamento, segundo o princípio do menor privilégio, de modo que cada participante acesse apenas o que é estritamente necessário às suas funções. Durante a habilitação, são configuradas as rotas autorizadas para cada participante, o que restringe no próprio gateway os endpoints acessíveis conforme a sua competência nos arranjos. Um PSP que atue por delegação opera somente dentro do escopo delegado, e as requisições a arranjos ou endpoints não autorizados **são recusadas antes do processamento**.

CAPÍTULO 5 – GESTÃO DE CERTIFICADOS E CHAVES

Este capítulo trata dos certificados e das chaves utilizados no Split Payment: os critérios técnicos que eles devem satisfazer, o seu ciclo de vida, a revogação em caso de comprometimento e a distribuição das chaves públicas pelo mecanismo de JWKS.

5.1 COMPATIBILIDADE TÉCNICA E HOMOLOGAÇÃO DE CERTIFICADOS

Os certificados utilizados na autenticação mTLS devem atender aos critérios de formato, algoritmos e cadeia de confiança apresentados a seguir, validados na homologação de segurança.

Item	Critério
Formato	Certificados digitais ICP-Brasil no padrão A1, no formato X.509, emitidos por autoridade certificadora reconhecida pela ICP-Brasil.
Algoritmos e Chaves	Compatibilidade mínima com certificados RSA 2048 bits e ECC P-256. Novas emissões devem priorizar algoritmos e tamanhos de chave compatíveis com as diretrizes de segurança vigentes da Plataforma Pública e da ICP-Brasil.
Cadeia de confiança	Deve ser realizada a validação completa da cadeia de certificação, incluindo certificados intermediários, autoridade certificadora raiz, período de validade, extensões de uso da chave e escopo de utilização do certificado.
Compatibilidade mTLS	Os certificados utilizados na autenticação mTLS devem atender aos requisitos técnicos definidos pela Plataforma Pública e possuir finalidade compatível com o processo de autenticação entre participantes.
Homologação	Os participantes devem validar cenários positivos e negativos de autenticação mTLS, incluindo certificado expirado, revogado, ausente, cadeia incompleta, ambiente incorreto, credencial não autorizada e demais cenários de falha previstos para o processo de integração.
Certificados da Plataforma Pública	Para a assinatura digital das mensagens, a Plataforma Pública utiliza certificado ICP-Brasil; para autenticação e criptografia da conexão, utiliza certificados SSL da cadeia v10 da ICP-Brasil.

5.2 CICLO DE VIDA E ROTAÇÃO

Os eventos de ciclo de vida e as ações obrigatórias associadas a cada um deles são os seguintes:

Evento	Ação obrigatória
Emissão	Validar participante, ambiente, escopo, cadeia e titularidade antes de ativar.
Renovação	Executar antes da expiração, com janela de convivência controlada.
Rotação ordinária	Certificados, chaves e respectivos registros publicados em JWKS possuem ciclo de vida formal, com renovação antecipada, atualização planejada e substituição com convivência, sem interrupção dos serviços.
Período de convivência	Prever coexistência entre certificados e chaves antigos e novos (dual key/dual certificate), permitindo migração controlada, validação em homologação e eventual reversão em caso de falhas.
Expiração	Rejeitar chamada com HTTP 401.

Evento	Ação obrigatória
Mudança de prestador	Revogar ou reemitir credenciais associadas à delegação encerrada.
Desabilitação da instituição	O desligamento de instituição, prestador de serviço ou escopo autorizado resulta em revogação dos certificados, remoção das chaves públicas do JWKS, atualização do JWKS e cancelamento das autorizações associadas.

5.3 REVOGAÇÃO E COMPROMETIMENTO

A revogação por suspeita de comprometimento exige três ações combinadas. A primeira é **revogar o certificado** ou a chave pelo mecanismo oficial, por CRL ou OCSP. A segunda é **remover a chave** do JWKS. A terceira é **invalidar os caches**, observando o SLA de propagação de revogação definido. A remoção do JWKS, isoladamente, não constitui revogação, pois as cópias em cache permanecem válidas até expirar.

O bloqueio de aceitação na Plataforma Pública deve ocorrer após a confirmação do comprometimento, sem depender da propagação externa de CRL ou OCSP. Em qualquer suspeita de comprometimento de certificados, chaves ou credenciais, as partes envolvidas são comunicadas imediatamente, com contenção, revogação, substituição e atualização dos registros publicados em JWKS. O tratamento de incidentes criptográficos é detalhado na Seção 7.2.

No desligamento de um participante ou de um PSP que opera por delegação, executa-se o processo de desabilitação, com a revogação de certificados, chaves, registros no JWKS, tokens, conectividade de rede (conforme o Manual de Redes), autorizações e delegações.

5.4 DISTRIBUIÇÃO DE CHAVES E CERTIFICADOS VIA JWKS

A distribuição e a atualização do material criptográfico público, tanto das chaves de assinatura digital (JWS) quanto do material de autenticação mútua (mTLS), são feitas por endpoints JWKS (JSON Web Key Set), conforme a RFC 7517. Cada participante mantém o seu próprio endpoint JWKS, previamente cadastrado no Portal da Reforma, e a Plataforma Pública publica as suas chaves públicas em endpoint JWKS próprio.

O JWKS transporta dois materiais distintos, cada um com finalidade própria. As **chaves de assinatura (JWS)** são as chaves públicas usadas para validar as assinaturas das mensagens, no uso tradicional do padrão, e serão identificadas pelo atributo "use: sig". Já o material de autenticação (mTLS) corresponde às **chaves públicas de autenticação mútua**, também expostas no JWKS por decisão de projeto da Plataforma Pública, sendo identificadas pelo atributo "use: tls". Ainda que a distribuição de material de mTLS por JWKS não seja o uso mais convencional do padrão, a opção é funcional e dispensa o cadastro e o envio manual de arquivos de certificados. A validação da cadeia X.509 e da ICP-Brasil segue os critérios da Seção 5.1.

A tabela a seguir descreve os endpoints JWKS do participante e da Plataforma Pública, a dinâmica de atualização e de rotação das chaves e a segregação por ambiente.

Elemento	Definição	Observação
Endpoint JWKS do participante	Cada participante expõe e mantém endpoint público protegido por HTTPS, contendo suas chaves	A URL do JWKS é informada à Plataforma Pública no Portal da Reforma na etapa de habilitação de

Elemento	Definição	Observação
	públicas de assinatura (JWS) e de autenticação (mTLS), por ambiente e por finalidade.	participantes; alterações de URL exigem atualização cadastral junto à gestão da Plataforma Pública.
Endpoint JWKS da Plataforma Pública	A Plataforma Pública publica suas chaves públicas em endpoint JWKS próprio, acessível aos participantes para validação de assinaturas e certificados da Plataforma Pública.	Endpoint disponibilizado no endereço: a definir
Atualização e rotação	A atualização de chaves é dinâmica: o participante publica a nova chave no JWKS e passa a utilizá-la, indicando o novo kid; a Plataforma Pública recupera automaticamente chaves desconhecidas a partir do endpoint. A recuperação automática observa controles de segurança obrigatórios: URL de JWKS em allowlist validada na habilitação de participantes, rate-limit de refetch, timeout de requisição, teto de número de chaves e de tamanho do keyset, e política de tratamento de colisão de kid entre participantes.	Cache, sobreposição de rotação e propagação de revogação seguem o definido na seção 6.2 (Requisitos JWS/JWT).
Segregação por ambiente	Homologação e produção utilizam endpoints JWKS, cadeias, escopos e certificados segregados.	Credenciais de homologação não são aceitas em produção e vice-versa.

Além dos elementos acima, o mecanismo de JWKS observa os requisitos funcionais de segurança descritos na tabela a seguir. Entre eles estão os controles de recuperação automática de chaves desconhecidas, como allowlist, limite de refetch, timeout, teto de chaves e tratamento de colisão de kid.

Requisito funcional	Descrição
Acesso autenticado	O acesso aos endpoints JWKS ocorre por HTTPS; a recuperação e o uso das chaves são associados ao participante correspondente.
Cadeia completa	Quando aplicável, devem ser disponibilizados o certificado, a CA intermediária e a CA raiz necessários à validação da cadeia X.509.
Metadados obrigatórios	Cada chave/certificado expõe kid, algoritmo, finalidade, validade e fingerprint, permitindo seleção e validação corretas.
Integridade	As respostas dos endpoints JWKS trafegam sob HTTPS e as chaves são validadas por kid e fingerprint; assinaturas e certificados são verificados conforme as seções 5 e 6.
Auditoria	Publicações, rotações, revogações e falhas de validação geram trilha auditável, registrando kid, fingerprint, ambiente e resultado.
Disponibilidade	O participante mantém seu endpoint JWKS em alta disponibilidade; indisponibilidade do endpoint impede a validação de mensagens assinadas com chaves ainda não propagadas.

CAPÍTULO 6 – ASSINATURA E INTEGRIDADE DE MENSAGENS

Este capítulo define o escopo da assinatura digital das mensagens e os requisitos técnicos de JWS e JWT que garantem a integridade, a autoria e o não repúdio do conteúdo.

6.1 ESCOPO DE ASSINATURA

A assinatura de payload complementa o mTLS. Enquanto o mTLS autentica o canal, a assinatura preserva a integridade, a autoria e o não repúdio do conteúdo, inclusive quando a mensagem passa por camadas internas, filas, prestadores ou reprocessamentos. A assinatura é transportada no header obrigatório indicado a seguir.

Header	Uso de segurança	Validação
X-JWS-Signature	Transporte da assinatura JWS detached (integridade e não repúdio).	Obrigatório nas rotas mutantes; JWS compact detached; corpo JSON idêntico ao usado no cálculo da assinatura.

Todas as funcionalidades da Plataforma Pública são assinadas, conforme a tabela abaixo:

Fluxo	Assinatura JWS
Informe de Transação Iniciada	Obrigatória.
Informe de Transação Atualizada	Obrigatória.
Informe de Baixa (exceto por pagamento)	Obrigatória.
Informe Preliminar de Pagamento	Obrigatória.
Informe de Segregação - início, lotes e finalização	Obrigatória.
Retorno Super Inteligente	Obrigatória.
Consulta Retroativa Super Inteligente	Obrigatória.
Mecanismo de Ocorrências (MOC)	Obrigatória.

6.2 REQUISITOS JWS/JWT

Os requisitos de formato, canonicalização, algoritmos, claims e validação da assinatura são apresentados a seguir. Assinatura inválida, kid desconhecido, certificado incompatível, claim divergente ou hash diferente resultam em rejeição.

Parâmetro	Valor definido
Formato de assinatura	JWS detached compact serialization, com hash do payload no header
Canonicalização JSON	JSON Canonicalization Scheme (JCS/RFC 8785) ou perfil equivalente definido pela PP.
Algoritmos permitidos	RS256 (RSASSA-PKCS1-v1_5 + SHA-256)
Claims mínimos	alg, typ, kid, b64, crit, jti, iat, hashPayload.

Parâmetro	Valor definido
Janela de expiração	A Plataforma Pública estabelece uma janela de até 5 minutos para a validade do jti. A tolerância de desvio de relógio (clock skew) na validação de iat é de até 1 minuto, com sincronização via NTP.
Validação bloqueante	Assinatura inválida, kid desconhecido, certificado incompatível, claim divergente ou hash diferente devem resultar em rejeição.

CAPÍTULO 7 – MONITORAÇÃO, REGISTRO, ALERTAS E RESPOSTA A INCIDENTES

Este capítulo reúne, de forma integrada, a classificação de incidentes, a observabilidade, os alertas, a resposta a incidentes e o registro de eventos de segurança. A classificação de incidentes (Seção 7.1) estabelece a escala de severidade utilizada pela tabela de sinais, alertas e resposta (Seção 7.2) e pelos eventos de log obrigatórios (Seção 7.3), que sustentam a rastreabilidade e as evidências (Seção 7.4).

7.1 CLASSIFICAÇÃO DE INCIDENTES

Os incidentes de segurança são classificados por severidade conforme o impacto técnico sobre a identidade, a integridade das mensagens, o sigilo dos dados e a disponibilidade. Essa escala é referenciada pelas seções seguintes, e os eventos concretos que disparam cada nível constam das tabelas das Seções 7.2 e 7.3.

Severidade	Critério definido
Crítica	Impacto real ou provável em Informe de Segregação, identidade institucional, vazamento relevante ou acesso indevido a dados de outro participante.
Alta	Falha de controle com potencial de impacto regulatório ou indisponibilidade em janela crítica.
Média	Falha sem impacto financeiro imediato, mas com risco operacional.
Baixa	Desvio controlado, sem impacto operacional ou de dados.

7.2 SINAIS MONITORADOS, ALERTAS E RESPOSTA

A tabela a seguir consolida, de forma integrada, os sinais e cenários monitorados, a severidade associada, a ação esperada e o prazo de comunicação. Incidentes envolvendo certificados, chaves privadas, PSK, JWKS, tokens de stream ou canais de distribuição de certificados são tratados como críticos, pois podem permitir usurpação de identidade, acesso indevido, adulteração de mensagens ou indisponibilidade dos informes.

Sinal ou cenário	Severidade	Ação esperada	Prazo de comunicação
Certificado mTLS próximo do vencimento	Alta	Alertas em D-30, D-15, D-7 e D-1; renovar o certificado antes do vencimento, com escalonamento automático se não houver renovação.	Não se aplica.
Certificado mTLS expirado, revogado, com cadeia inválida ou comprometido	Crítica	Alerta crítico imediato ao NOC/SOC, com bloqueio ou rejeição da chamada. Suspender ou restringir o certificado, revogar pelo mecanismo definido, emitir novo certificado e validar participante e arranjos antes do retorno.	Em até 1 hora após a suspeita qualificada.
cnpjRaizPspRecDir incompatível com o certificado em stream	Crítica	Alerta crítico e bloqueio da operação.	Não se aplica.
Cipher Suite fora do padrão	Alta	Alerta e abertura de desvio de configuração.	Não se aplica.

Sinal ou cenário	Severidade	Ação esperada	Prazo de comunicação
Falhas repetidas de handshake TLS/mTLS	Alta	Alerta correlacionado por participante, IP, certificado e endpoint, com investigação da origem das falhas.	Não se aplica.
Falha de CRL, OCSP ou JWKS, ou cache expirado	Alta	Alerta, acionamento de contingência e registro de evidência de indisponibilidade.	Não se aplica.
Falha repetida de assinatura JWS, inclusive no Retorno Super Inteligente	Alta	Alerta e, ao atingir 5 ocorrências em 10 minutos, escalonamento crítico.	Não se aplica.
Chave privada JWS comprometida	Crítica	Alerta crítico. Revogar o kid no JWKS, bloquear a aceitação de assinaturas antigas fora da janela autorizada, republicar o JWKS e reprocessar as evidências afetadas.	Em até 30 minutos para a comunicação inicial.
Credencial de conectividade de rede exposta	Crítica	Alerta crítico. Rotacionar a credencial, revisar o acesso de rede conforme o Manual de Redes e investigar uso indevido.	Em até 30 minutos para a comunicação inicial.
Acesso indevido a dados de outro participante confirmado	Crítica	Alerta crítico e contenção imediata do acesso, com tratamento como incidente crítico.	Notificação imediata, com contenção em até 1 hora.
Vazamento de dados fiscais ou pessoais	Crítica	Alerta crítico e acionamento do plano de resposta a incidentes e das partes definidas.	Em até 24 horas, conforme as obrigações legais aplicáveis.

Quando um PSP que opera por delegação identifica um incidente, notifica imediatamente o PSP Recebedor Direto, que responde perante a Plataforma Pública nos prazos indicados. As obrigações formais de notificação e os aspectos de habilitação e desabilitação de participantes são detalhados no Manual de Habilitação de Participantes.

7.3 EVENTOS DE LOG OBRIGATÓRIOS

Os eventos listados a seguir são de registro obrigatório, com a severidade mínima e o destino indicados. Eles se relacionam diretamente com os sinais e as ações de resposta da Seção 7.2, e observam o mascaramento de dados sensíveis e o envio ao SIEM.

Evento	Severidade mínima	Destino
Falha mTLS	Alta	SIEM/SOC
Falha JWS	Alta	SIEM/SOC
Tentativa de acesso indevido a dados de outro participante	Crítica	SIEM/SOC + incidente
jti com payload divergente	Alta	SIEM/SOC
Revogação de certificado/chave	Alta	SIEM/SOC + auditoria

7.4 RASTREABILIDADE E EVIDÊNCIAS

Toda decisão crítica de segurança gera registro auditável, correlacionável e protegido contra alteração, de modo que a autoria, a integridade e o horário possam ser demonstrados posteriormente. As evidências relevantes, como identificadores de remessas e resultados de validação, são preservadas pelos prazos aplicáveis, e os registros são correlacionáveis no escopo de atuação da PPS para a investigação de incidentes e a comprovação de conformidade.

CAPÍTULO 8 – HISTÓRICO DE REVISÃO

Data	Versão	Descrição das Alterações
27/07/2026	1.0.0	Versão Inicial

APÊNDICE A - GLOSSÁRIO DE SEGURANÇA

Termo	Definição
Cipher Suite	Conjunto de algoritmos negociados em TLS para troca de chaves, autenticação, cifragem e integridade.
CRL/OCSP	Mecanismos de verificação de revogação de certificados digitais.
HSM	Módulo criptográfico de hardware utilizado para proteger chaves e executar operações criptográficas controladas.
IGA	Índice Geral de ANS (Acordo de nível de serviço)
JWKS	JSON Web Key Set; conjunto de chaves públicas para validação de assinaturas.
JWS	JSON Web Signature; mecanismo para assinar conteúdo JSON.
kid	Identificador da chave usada em uma assinatura.
KMS	Serviço de gestão de chaves criptográficas com políticas de acesso, rotação e auditoria.
mTLS	Autenticação mútua TLS por certificado de cliente e servidor.
Perfect Forward Secrecy (PFS)	Propriedade que impede que o comprometimento futuro de uma chave privada permita descriptografar sessões antigas.
Portal da Reforma (GOV.BR)	Área autenticada via GOV.BR, no Portal da Reforma, utilizada para publicação e download de certificados públicos e cadeias.
PSK	Pre-Shared Key usada para autenticação do túnel IPsec.
TLS Passthrough	Encaminhamento da sessão TLS até o serviço de destino, sem terminação no intermediário.
TLS Termination	Encerramento da sessão TLS em componente intermediário, como API Gateway, Load Balancer ou Reverse Proxy.
Vault ou cofre de segredos	Repositório seguro para segredos, PSKs, credenciais e chaves, com controle de acesso e trilha de auditoria.

APÊNDICE B - MATRIZ DE CONTROLES POR ATOR

A matriz resume a responsabilidade por controle. A coluna “PSP por delegação” refere-se ao PSP que opera em nome de outro participante, por exemplo prestando o serviço de conexão, e que permanece sujeito aos controles deste manual dentro do escopo delegado.

Controle	PP	PSP Recebedor Direto / Núclea	PSP por delegação
mTLS	Valida certificado	Protege certificado e chave	Protege se delegado
JWS/JWKS	Valida/assina conforme fluxo	Assina requisições e valida respostas	Assina se delegado
Autorização	Decide e aplica	Solicita escopo correto	Opera apenas escopo
Logs	Registra lado PP	Registra lado participante	Registra execução
Incidentes	Bloqueia/restaura Plataforma Pública	Contém/notifica/corrige	Notifica e contém