Receita Federal

Manual de Preenchimento e-Financeira

Manual de Orientação do Desenvolvedor

Versão 2.5

Outubro/2025

ORIENTAÇÕES PARA PREENCHIMENTO DA E-FINANCEIRA

Este documento é parte do Manual da e-Financeira, ele contém as Orientações ao Desenvolvedor.

Histórico de Alterações

Versão	Data	Alterações	Seção impactada
2.0	24/09/2024	Versão inicial	
2.1	07/11/2024	Alteração na redação: "*O quantidade máxima permitida será de 100 eventos por lote*" substituído por "*A quantidade máxima permitida será de 100 eventos por lote do modo síncrono, e 50 eventos por lote do modo assíncrono*".	Estrutura, Dados Técnicos e Definições
2.1	07/11/2024	Alteração no tamanho máximo da mensagem permitida: "**80 MB**" substituído por "**60 MB**".	Transmissão de Lotes - Modo Assíncrono
2.1	07/11/2024	Parâmetros **tipoIdentificacao** e **identificacao** em todas as Consultas Informações de Movimento (Operação Financeira, Operação Financeira Anual, Previdência Privada, Repasse) alterados de Obrigatório "**N**" para "**S**".	Consulta das informações enviadas em Eventos
2.2	13/12/2024	Adicionada Seção “Transmissão de Lotes e Consultas - Modo Síncrono”	Transmissão de Lotes e Consultas - Modo Síncrono
2.3	20/12/2024	Atualizadas informações relativas à limitação de quantidade de eventos e limpeza dos dados no ambiente de testes (produção restrita)	"Transmissão Lotes – Ambiente Testes (Produção Restrita)" e "Endpoint para Limpeza de dados no Ambiente de Testes (Produção Restrita)"
2.4	17/01/2025	Removidas informações relativas aos eventos de Repasse	Todo o manual
2.4	01/03/2025	Sem mudanças em conteúdo, apenas na capa.	Capa
2.5	16/10/2025	Removido conteúdo relativo ao modo síncrono	Todo o manual

Sumário

1. ESTRUTURA, DADOS TÉCNICOS E DEFINIÇÕES 6
   1.1. Lotes e Eventos 6
   1.2. Fluxo de Envio dos Dados 6
   1.3. Assinatura e Processamento 6
   1.4. Níveis de Validação 7
   1.5. Padrão de Documento XML 7
   1.5.1. Declaração Namespace 8
   1.5.2. Schema 8
   1.6. Padrão de Comunicação 9
   1.7. Padrão de Certificado Digital 9
   1.8. Padrão de Assinatura Digital 10
   1.8.1. Processo de Validação da Assinatura Digital 11
   1.9. Resumo dos Padrões Técnicos 12
2. ESTRUTURAS / SCHEMAS / XSD 12
   2.1. Tipos de Schema 13
   2.2. Validação da Estrutura 13
3. EVENTOS 13
   3.1. Estrutura do Evento 14
   3.2. Identificação do Evento 14
   3.3. Versionamento dos Leiautes dos Eventos 15
   3.4. Definições dos Leiautes 15
   3.5. Status dos eventos e da e-Financeira 16
4. LOTES - CRIPTOGRAFIA E COMPACTAÇÃO 16
   4.1. Criptografia de Lotes 16
   4.1.1. Modelo de Criptografia 17
   4.1.2. Fluxo para Geração e Envio de Lotes Criptografados 17
   4.1.3. Passos geração Chave e Lote criptografado 18
   4.1.4. Padrões criptografia Lotes e-Financeira 18
   4.1.5. Mensagens específicas para inconsistência em Lote Criptografado 18
   4.2. Compactação de Lotes 19
   4.2.1. Modelo de Compactação Gzip 19
   4.2.2. Processo para Geração de um Lote Criptografado e Compactado Gzip 19
5. TRANSMISSÃO DE LOTES - MODO ASSÍNCRONO 19
   5.1. API REST para Transmissão de Lote 20
   5.2. Processo de Transmissão de Lote no modo Assíncrono 20
   5.3. Códigos retorno HTTP previstos para a API de Recepção 21
   5.4. Retorno Recepção XML Lote modo Assíncrono e tag cdResposta 21
   5.5. API REST para Consulta do Processamento de Lote 21
   5.6. Processo de Consulta do Processamento de Lote no modo Assíncrono 22
   5.7. Códigos retorno HTTP previstos para a API de Consulta de Lote no modo Assíncrono 22
   5.8. Retorno Consulta de Lote no modo Assíncrono e tag cdResposta 23
   5.9. Uso abusivo de Consultas / rate limiting 23
6. TRANSMISSÃO LOTES – AMBIENTE DE TESTES (PRODUÇÃO RESTRITA) 23

7. CONSULTA DAS INFORMAÇÕES ENVIADAS EM EVENTOS....24
7.1.1. API REST para Consultas de dados enviados em Eventos....24
7.2. Parâmetros das Consultas....26
7.3. Retorno solicitação consulta e tag cdResposta....29
7.4. Códigos retorno HTTP previstos para a API de Consulta....30
8. ENDPOINT PARA LIMPEZA DE DADOS NO AMBIENTE DE TESTES (PRODUÇÃO RESTRITA)....30
9. RECOMENDAÇÕES E BOAS PRÁTICAS....31
9.1. Otimizar a montagem do arquivo....31
9.2. Eventos de movimento com muitas contas....31
9.3. Evitar consultas repetidas em excesso....32
9.4. Aguardar para iniciar a consulta ao protocolo de um Lote no modo Assíncrono....32
9.5. Enviar evento de 'Fechamento' em Lote separado, e somente após finalizar todo o envio de eventos de Movimento....32
9.6. Ambiente de Testes - Produção Restrita : Exclusão automática dos dados a cada fim de semestre....32

1. Estrutura, Dados Técnicos e Definições

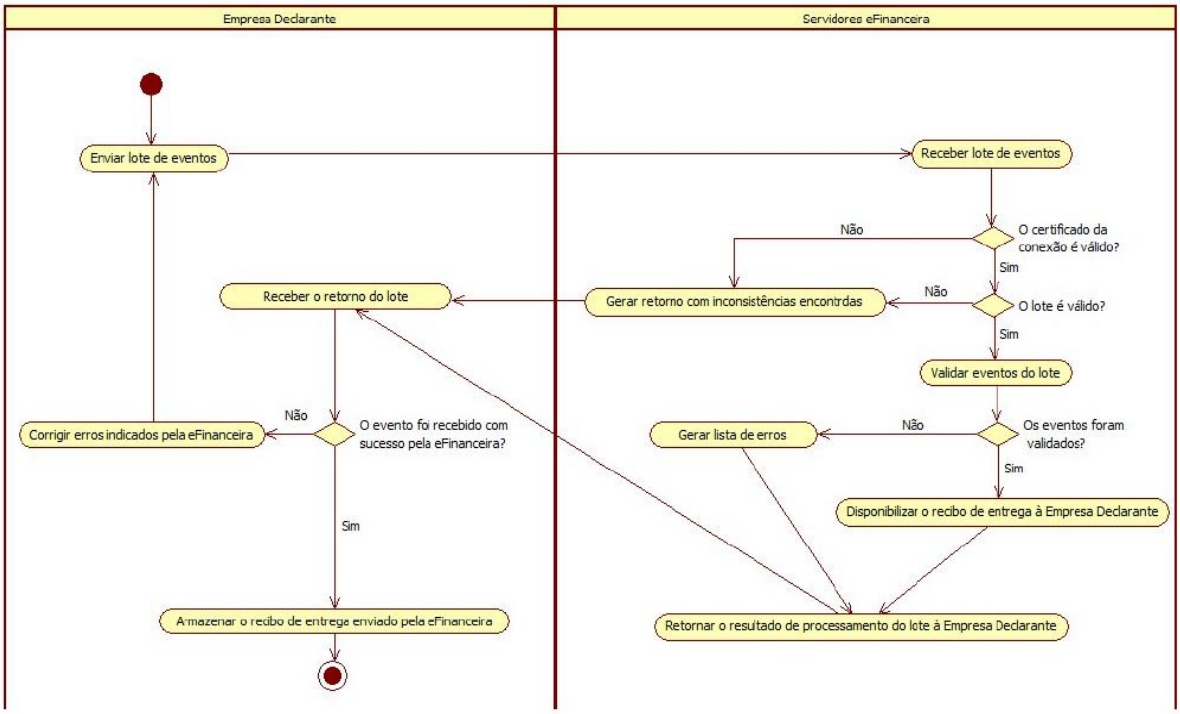
1.1. Lotes e Eventos

As informações serão fornecidas pela instituição declarante por meio de arquivo(s) **XML de Evento**, enviado(s) dentro de um **XML de Lote.**

O **XML de Lote** deverá ser enviado através de *API REST (modo assíncrono)*.

A quantidade máxima permitida será de 50 eventos por lote do modo assíncrono. No Ambiente Nacional, os eventos serão extraídos dos lotes, e submetidos a validações quanto à estrutura e ao conteúdo e em relação a outros eventos recebidos anteriormente, garantindo a qualidade da informação.

1.2. Fluxo de Envio dos Dados



O processamento dos eventos recebidos será executado de assíncrona, com a envio e a consulta de Lotes sendo feitos via APIs REST.

No modo assíncrono, o processamento será executado assíncronamente e o declarante receberá um protocolo para consulta futura ao resultado do lote.

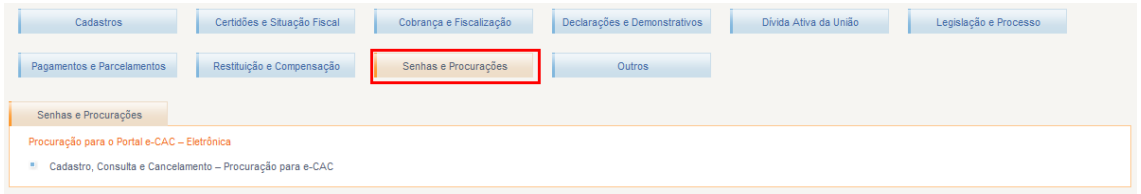
Cada evento dentro do lote que tiver sucesso no envio e no processamento de estrutura e conteúdo receberá um número de recibo, que deve ser armazenado pelo declarante.

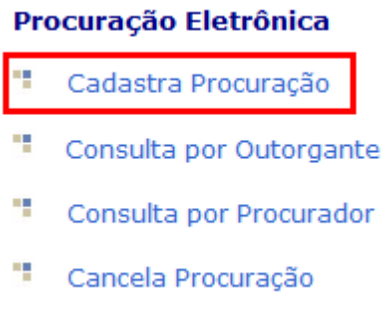
O sistema possui também serviços específicos para consultas, onde é possível obter informações das empresas declarantes, informações de movimentos, de intermediários e de patrocinados, bem como a relação dos arquivos eletrônicos enviados por cada instituição.

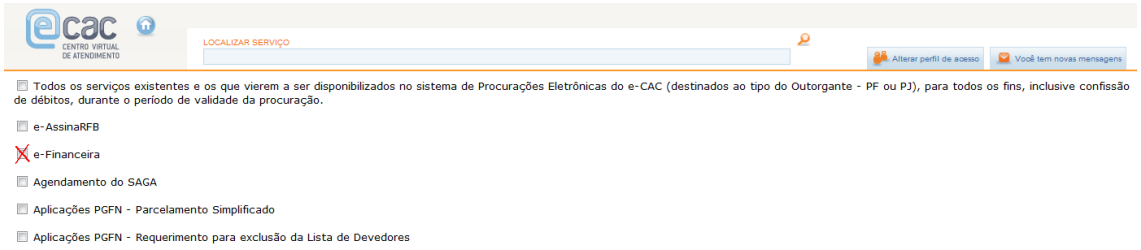
1.3. Assinatura e Processamento

Os arquivos XML de evento deverão ser assinados digitalmente, nos termos da legislação brasileira, de modo a garantir a integridade dos dados e a autoria do emissor.

ATENÇÃO : Os eventos deverão ser assinados digitalmente utilizando o e-CNPJ da entidade, e-aplicação ou e-CPF de seu representante legal ou procurador. Neste último caso, a procuração eletrônica para a pessoa física deverá ser cadastrada no portal do e-CAC, utilizando o acesso via certificado digital e indicando, especificamente, poderes referentes à e-Financeira.







1.4. Níveis de Validação

1. Validação do Lote: executada no momento da recepção do lote de eventos, quando serão verificados, inicialmente, o certificado da conexão e a estrutura e versão do lote. Caso ocorra erro na validação do lote, o lote não será recebido e não serão realizadas as validações dos eventos, descritas abaixo.

2. Validação dos Eventos contidos no Lote

Para cada evento contido no lote, serão feitas as seguintes validações:

- Validação de estrutura: validação do evento em relação à estrutura do arquivo, de acordo com o tipo de evento. Caso ocorra erro na validação de estrutura, o evento não será recebido e não serão realizadas as demais validações do evento.

- Validação de conteúdo: validações dos valores informados no evento. Caso seja detectada alguma inconsistência, o evento não será recebido.

1.5. Padrão de Documento XML

A especificação do documento XML adotada é a recomendação W3C para XML 1.0, disponível em http://www.w3.org/TR/REC-xml.

A codificação dos caracteres será em UTF-8 e assim, todos os documentos XML devem ser iniciados com a seguinte declaração:

<?xml version="1.0" encoding="UTF-8"?>

Um arquivo XML poderá ter uma única declaração *<?xml version="1.0" encoding="UTF-8"?>*. Mesmo nas situações em que um documento XML contenha outros documentos XML, como ocorre no documento de Lotes de Eventos, deve-se atentar para que exista uma única declaração no início do documento.

Alguns caracteres especiais são proibidos, para não gerar erros na codificação do documento enviado ao sistema. Será necessário substituir os caracteres especiais pelas sequências de caracteres de escape adequados, conforme tabela abaixo. Os caracteres que não possuírem informações na coluna de "escape" devem ser eliminados do arquivo original:

Caractere	**Escape**
> (sinal de maior)	>
< (sinal de menor)	<
& (e comercial)	&
” (aspas duplas)	
’ (sinal de apóstrofe ou aspas simples)	
--	
#	

1.5.1. Declaração Namespace

Cada evento XML deverá ter uma única declaração de *namespace* no elemento raiz do documento, de acordo com o tipo de evento enviado, e com o seguinte padrão:

```
<xmlns="http://www.eFinanceira.gov.br/schemas/xxxxxxxx/vY_Y_Y"
```

Onde "xxxxxxxx" é o tipo do evento enviado, conforme o leiaute vigente para a e-Financeira. É vedado o uso de declaração de *namespace* diferente do padrão estabelecido.

A parte referente à versão do leiaute (vY_Y_Y) deve ser atualizada sempre que necessário, quando houver atualizações do Schema (.XSD).

A declaração do *namespace* da assinatura digital deverá ser realizada na própria tag <Signature>, conforme exemplo abaixo:

```
<xmlns=”http://www.eFinanceira.gov.br/schemas/xxxxxxxx/vY_Y_Y”>
<!-- Xml do Evento -->
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<.../>
</Signature>
</eFinanceira>
```

1.5.2. Schema

A estrutura dos arquivos XML recebidos pela e-Financeira é especificada e checada por um *Schema*, linguagem que define a estrutura do documento XML, descreve seus elementos e sua organização, estabelecendo as regras de preenchimento de conteúdo e de obrigatoriedade de cada elemento ou grupo de informação. Este *Schema* é representado fisicamente por um arquivo de extensão XSD.

A validação da estrutura XML da mensagem é realizada por um analisador sintático (parser) que verifica se a mensagem atende as definições e as regras de seu *Schema*. Qualquer divergência da estrutura XML da mensagem, em relação ao seu *Schema*, provocará erro de validação de estrutura.

1.6. Padrão de Comunicação

A comunicação será baseada em *APIs REST (modo assíncrono)*, disponibilizados pelo Serpro.

O meio físico de comunicação utilizado será a Internet, com o uso do protocolo HTTPS (TLS 1.2), com autenticação mútua, que, além de garantir um duto de comunicação seguro na Internet, permite a identificação do servidor e do cliente através de certificados digitais.

1.7. Padrão de Certificado Digital

O certificado digital utilizado na e-Financeira deverá ser emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

O certificado digital deverá pertencer à série A. Existem duas séries às quais os certificados podem pertencer: a série A e a série S. A série A reúne os certificados de assinatura digital utilizados na confirmação de identidade na Web, em e-mails, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações. A série S reúne os certificados de sigilo que são utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.

O certificado digital deverá ser do tipo A1 ou A3. Certificados digitais de tipo A1 ficam armazenados no próprio computador utilizado. Certificados digitais do tipo A3 são armazenados em dispositivos portáteis invioláveis do tipo smart card ou token, que possuem um chip com capacidade de realizar a assinatura digital. Este tipo de dispositivo é bastante seguro, pois toda operação é realizada pelo chip existente no dispositivo, sem qualquer acesso externo à chave privada do certificado digital.

Para que um certificado seja aceito na função de transmissor de solicitações este deverá ser do tipo e-aplicação, e-CPF (e-PF) ou e-CNPJ (e-PJ).

Os certificados digitais podem ser utilizados tanto nas conexões SSL de transmissão dos lotes de eventos para a e-Financeira, quanto para a assinatura dos eventos. Neste caso, os efeitos da validação podem ser para todo o lote (no caso de o erro ser gerado a partir do certificado de transmissão) como para um evento específico (no caso do erro ser gerado a partir da assinatura de um documento XML enviado para a e-Financeira que representa o evento).

Transmissão: antes de ser iniciada a transmissão de solicitações ao sistema, o certificado digital do solicitante é utilizado para reconhecer o transmissor e garantir a segurança do tráfego das informações na Internet.

Assinatura de documentos: para garantir o não repúdio e a integridade das informações, os documentos eletrônicos enviados para a e-Financeira são assinados digitalmente seguindo a especificação descrita no item “Padrão de Assinatura Digital” e nas orientações estabelecidas neste manual.

Os Certificados Digitais utilizados no acesso aos serviços disponibilizados pelo sistema e na assinatura dos arquivos XML enviados deverão atender aos seguintes critérios:

Critério	Mensagem	Efeito
A formação da cadeia de certificação até sua raiz deve ser confiável	MS0003	Rejeição do lote ou do evento
A raiz da cadeia deverá pertencer a Autoridade Certificadora Raiz Brasileira (ICP-Brasil)	MS0004	Rejeição do lote ou do evento
O certificado não poderá estar revogado	MS0005	Rejeição do lote ou do evento
O certificado não poderá estar expirado na data da verificação	MS0006	Rejeição do lote ou do evento
O certificado deverá ser do tipo e-aplicação, e-CNPJ, e-PJ, e-CPF ou e-PF	MS0007	Rejeição do lote ou do evento
O certificado digital utilizado para assinatura deve p ossuir os atributos 'digitalSignature' e 'nonRepudiatio n' em sua chave 'Key Usage' (uso da chave).	MS1208	Rejeição do evento

1.8. Padrão de Assinatura Digital

O sistema utiliza um subconjunto do padrão de assinatura XML, definido pelo http://www.w3.org/TR/xmldsig-core/.

A assinatura digital do documento eletrônico deverá ser realizada na tag do XML que contém o atributo "ID" e deve atender aos seguintes padrões adotados:

- **Padrão de assinatura**: *XML Digital Signature*, utilizando o formato *Enveloped* (http://www.w3.org/TR/xmldsig-core/)

- Certificado digital: emitido por AC credenciada no ICP-Brasil (http://www.w3.org/2000/09/xmldsig#X509Data)

- **Cadeia de certificação**: *EndCertOnly* (Incluir na assinatura apenas o certificado do usuário final)

- **Tipo do certificado**: A1 ou A3

- **Tamanho da chave criptográfica**: compatível com os certificados A1 e A3 (1024 e 2048 bits).

- **Função criptográfica assimétrica**: RSA (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)

- **Função de *message digest***: SHA-2 (http://www.w3.org/2001/04/xmlenc#sha256)

- **Codificação**: Base64 (http://www.w3.org/2000/09/xmldsig#base64)

- **Transformações exigidas**: útil para realizar a canonicalização do XML enviado, para realizar a validação correta da assinatura digital. São elas:

- *Enveloped* (http://www.w3.org/2000/09/xmldsig#enveloped-signature)

- *C14N* (http://www.w3.org/TR/2001/REC-xml-c14n-20010315)

As informações necessárias à identificação do assinante estão presentes dentro do certificado digital, tornando desnecessária a sua representação individualizada no arquivo XML. Portanto, o arquivo XML assinado deverá conter apenas a tag *X509Certificate* nas informações que dizem respeito ao certificado.

Abaixo temos um exemplo de um evento assinado digitalmente, onde xxxxxxx é o nome do evento enviado:

```
<?xml version="1.0" encoding="UTF-8"?>
<eFinanceira xmlns="http://www.eFinanceira.gov.br/schemas/ xxxxxxx /v1_2_0">
<!-- Xml do Evento Aqui -->
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
  <Reference URI="#ID1000000004929321">
   <Transforms>
    <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
   <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
   <DigestValue>fLTJL1BLGP9giKdsEGP9xSVyeWBlPzkvyy78GtbsC9I=</DigestValue>
  </Reference>
 </SignedInfo>
 <SignatureValue>GfFvpoo2Q .... +6aQ==</SignatureValue>
 <KeyInfo>
  <X509Data>
   <X509Certificate>MIIHVDCCBTygAwIBAgIQM..... LoOUSyCgU=</X509Certificate>
  </X509Data>
 </KeyInfo>
 </Signature>
</eFinanceira>
```

Conforme a Resolução 179 de 20/10/2020, do Comitê Gestor da ICP Brasil, no item 7.1.2.7 inciso b, os certificados de autenticação de servidor (SSL/TLS) não podem mais ter o atributo "não repúdio" habilitado. Sendo assim, os certificados de raiz v10 que não possuírem esse atributo devem ser utilizados apenas para autenticação, evitando-se o seu uso para assinaturas digitais.

1.8.1. Processo de Validação da Assinatura Digital

O Procedimento de validação da assinatura digital adotado pelo sistema da e-Financeira é:

1. extrair a chave pública do certificado;

2. verificar o prazo de validade do certificado utilizado;

3. montar e validar a cadeia de confiança dos certificados, validando também a LCR (Lista de Certificados Revogados) de cada certificado da cadeia;

4. validar o uso da chave utilizada (assinatura digital) de forma a aceitar certificados somente do tipo A (não serão aceitos certificados do tipo S);

5. garantir que o certificado utilizado é de um usuário final e não de uma autoridade certificadora;

6. adotar as regras definidas pelo RFC 3280 para as LCR e cadeia de confiança;

7. validar a integridade de todas as LCR utilizadas pelo sistema;

8. verificar data inicial e final do prazo de validade de cada LCR utilizada.

1.9. Resumo dos Padrões Técnicos

A tabela a seguir resume os principais padrões de tecnologia utilizados:

Característica	Descrição
API REST	Serviço que segue o padrão REST (Representational State Transfer)
Meio físico de comunicação	INTERNET
Protocolo	HTTPS (SSL versão 3.0), com autenticação mútua através de certificados digitais.
Padrão da mensagem	XML no padrão Style/Encoding: Document/Literal
Padrão de certificado digital	X.509 versão 3, emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, do tipo A1 ou A3, devendo ser e-aplicação, e-CPF (e-PF) ou e-CNPJ (e-PJ). Para transmissão, utilizar o certificado digital do responsável pela transmissão.
Padrão de assinatura digital	XML Digital Signature, Enveloped, com certificado digital X.509 versão 3, com chave privada de tamanho variável, conforme o padrão da ICP-Brasil (1024, 2048, ou mais bits), com padrões de criptografia assimétrica RSA, algoritmo message digest SHA-2 e utilização das transformações Enveloped e C14N.
Validação de assinatura digital	Será validada além da integridade e autoria, a cadeia de confiança com a validação das LCR.
Padrões de preenchimento XML	Campos não obrigatórios do *Schema* que não possuam conteúdo devem ter suas tags suprimidas no arquivo XML
	Nos campos numéricos inteiros, não incluir vírgula ou ponto decimal.
	Nos campos numéricos com casas decimais, utilizar a vírgula na separação das casas decimais, observando a definição do leiaute específico do evento a ser enviado.

2. Estruturas / Schemas / XSD

Os *Schemas* (XSD) que definem os XML aceitos serão disponibilizados via Portal do SPED.

Endereço : http://sped.rfb.gov.br/pasta/show/1500

2.1. *Tipos de Schema*

Existem os seguintes pacotes de *Schemas*:

- **Comunicação**: contém os *Schemas* envolvidos no processo de comunicação com o sistema da e-Financeira:
    - Envio Lote Criptografado (modo assíncrono)
    - Retorno de Lote (modo assíncrono)
    - Retorno de Evento
    - Retorno de Solicitacao de Consulta Assíncrona
    - Schema padrão Assinatura Digital (xmldsig-core-schema)
- **Eventos**: contém os *Schemas* para cada evento de negócio previstos para serem enviados para a e-Financeira.
- **Consulta**: contém os *Schemas* para o retorno das consultas previstas para a e-Financeira

2.2. *Validação da Estrutura*

As aplicações que fazem solicitações ao sistema da e-Financeira devem estar preparadas para gerar XMLs no formato definido pelo Schema em vigor.

As alterações da estrutura de dados XML realizadas nas mensagens são controladas através da versão definida no namespace do Schema. A identificação da versão dos Schemas será realizada com o acréscimo do número da versão como sufixo no namespace do XML e no nome do arquivo, como se segue:

Exemplo em namespace (evento movimentação) :
*http://www.efinanceira.gov.br/schema/evtMovOpFin/**v1_2_1***

Exemplo em nome arquivo xsd (lote) :
*envioLoteEventos-**v1_2_0**.xsd*

As modificações de leiaute podem ser causadas por necessidades técnicas ou em razão da modificação de alguma legislação. Quando decorrente de alterações da legislação, deverão ser implementadas nos prazos previstos no ato normativo que introduziu a alteração. As modificações de ordem técnica serão divulgadas no Portal do SPED pela Coordenação Técnica do Sistema e ocorrerão sempre que atualizações forem necessárias.

3. Eventos

As informações relativas à elaboração dos documentos XML, contendo o Evento e o Retorno do processamento do Evento estão detalhadas abaixo.

3.1. Estrutura *do Evento*

Cada evento tem sua própria estrutura. A verificação da estrutura dos eventos, conforme os seus respectivos leiautes, será realizada através de seu Schema XSD.

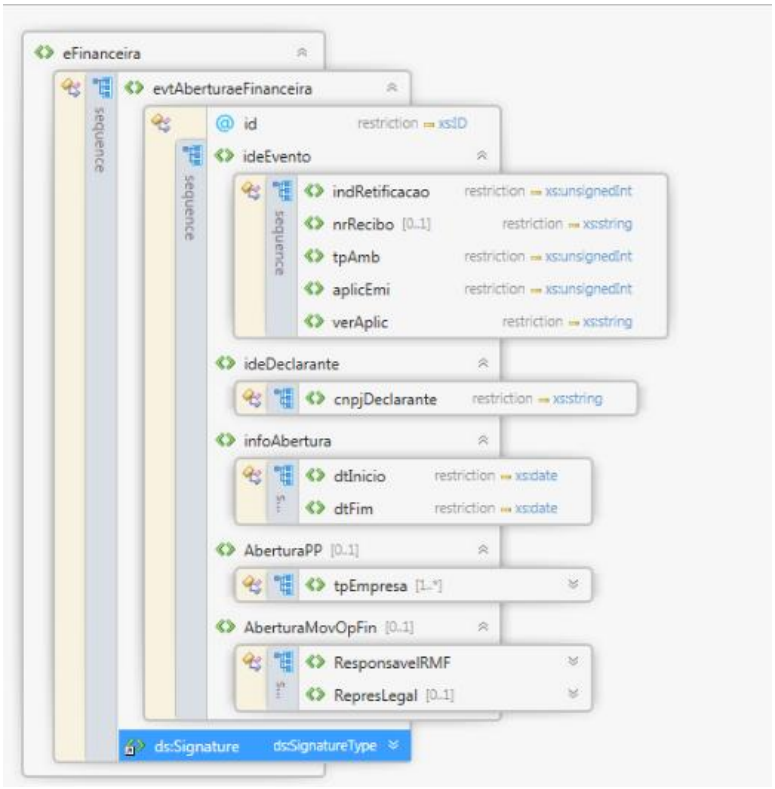
Cada XSD que representa o leiaute de um evento tem o seu próprio *Namespace* que identifica o tipo de evento e versão.

Exemplo : Evento de Abertura

http://www.eFinanceira.gov.br/schemas/evtAberturaEFinanceira/v1_2_0

http://www.eFinanceira.gov.br/schemas/	Estabelece que o XSD é de um evento do eFinanceira.
evtAberturaEFinanceira	Identificação do Tipo do evento.
v1_2_0	Identificação da versão do Leiaute

Estrutura básica do evento :



3.2. Identificação do Evento

Cada evento da e-Financeira possui uma identificação única, gerada pela própria entidade declarante, conforme padrão abaixo:

Campo Fixo	**Sequencial**

ID	Número sequencial
2 posições	18 posições

Exemplo: ID233390170000000000 (20 posições).

Deve representar unicamente o evento no sistema para a mesma entidade declarante e mesmo tipo de evento.

3.3. Versionamento *dos Leiautes dos Eventos*

O versionamento dos leiautes dos eventos será por tipo de evento. A alteração do leiaute de um determinado tipo de evento não afeta a versão dos demais tipos de eventos.

Seguem abaixo os princípios que serão considerados no versionamento dos leiautes:

- O leiaute do tipo de evento compreende apenas a sua estrutura. O mesmo leiaute poderá ter um conjunto diferente de regras e valores válidos durante o seu período de vigência. A alteração dos valores válidos ou do conjunto de regras de um leiaute, sem alteração de sua estrutura, será realizada através da atualização deste Manual, sem a necessidade de alteração da versão do leiaute.

- Para cada tipo de evento haverá apenas uma versão de leiaute vigente em um determinado período.

- Cada XSD é identificado por um único *Namespace* e cada XSD representa apenas um leiaute.

- A e-Financeira identificará a versão do leiaute do evento através do *namespace* do XML do evento.

Identificação da versão de Leiaute (**X.Y**) e *Schema* XML - XSD (**X**_**Y**_**Z**)

Em que:

X -> utilizado para representar mudanças muito significativas (Reestruturação do evento)

Y -> utilizado para representar mudanças estruturais comuns (Inclusão/exclusão de campos, dentre outras).

Z -> utilizados para corrigir erros em XSD publicados e possivelmente, já utilizados. Neste caso, haverá uma substituição do "pacote de liberação" do referido período.

3.4. Definições dos Leiautes

O arquivo do Evento é um arquivo XML formado por elementos que contém os dados e são reunidos em grupos que, por sua vez, possuem uma hierarquia entre si.

Os elementos podem ser definidos como:

ELEMENTO
G = Grupo
A = Atributo
E = Elemento

Os registros possuem uma regra de ocorrência e obrigatoriedade, conforme as legendas abaixo.

OCORRÊNCIA
1-1 = O registro deve ocorrer uma única vez no arquivo
0-1 = O registro pode ocorrer uma ou nenhuma vez no arquivo
1-N = O registro pode ocorrer uma ou mais vezes
0-N = O registro pode ocorrer nenhuma ou várias vezes no arquivo

OBRIGATORIEDADE
O = REGISTRO OBRIGATÓRIO
OC = REGISTRO OBRIGATÓRIO SE HOUVER
O(...) = REGISTRO OBRIGATÓRIO EM FUNÇÃO DE UMA CONDIÇÃO
N = REGISTRO NÃO DEVE SER INFORMADO

As regras de validação que se referem a conferência de campos que se encontram em outros registros somente serão executadas se o registro referenciado puder existir, ou seja, sua obrigatoriedade terá que ser diferente de “N”.

Quando informado grupo facultativo, deverá ser obedecida a obrigatoriedade de campos apresentados.

3.5. Status dos eventos e da e-Financeira

Ao serem transmitidos, os eventos recebem um número de recibo para controle do declarante e adquirem um status (EXCLUÍDO, RETIFICADO, ATIVO) no banco de dados do servidor da e-Financeira.

Os eventos nunca são apagados do banco de dados. Se um deles for retificado ou excluído, ele terá o status alterado e poderá sempre ser consultado.

A e-financeira , da mesma forma, após o envio do evento de abertura, eventos de movimento e evento de fechamento possui um status para acompanhamento (EM ANDAMENTO, EXCLUÍDA, ATIVA)**.**

Maiores detalhamentos sobre este item estão descritos no Manual e-financeira no item 1.7.2.1.4.

4. Lotes - Criptografia e Compactação

4.1. Criptografia de Lotes

Conforme artigo 2º do Ato Declaratório Executivo COFIS nºXX, de 05 de maio de 2017, a utilização desse modelo de criptografia de dados da e-Financeira passa a ser obrigatória para quaisquer arquivos transmitidos a partir do primeiro dia útil de março de 2018, inclusive para enviar retificações de arquivos transmitidos/a serem transmitidos sem criptografia até o último

dia útil de fevereiro de 2018 (data final para a possibilidade de transmissão de arquivos da e-Financeira sem criptografia dos dados).

4.1.1. Modelo de Criptografia

Esse modelo possibilita que os dados sejam criptografados, ainda no disco da Instituição Financeira, para serem enviados ao servidor do e-Financeira. O envio deste arquivo será realizado sobre o túnel criptografado TLS 1.2.

A abordagem de criptografia híbrida foi escolhida para possibilitar que a solução possua performance nas operações de cifragem/decifragem dos arquivos e também possa ser possível compartilhar a chave de criptografia entre o servidor e o cliente de forma segura.

Neste esquema de criptografia utiliza-se um algoritmo de chave simétrica para criptografar a mensagem a ser enviada. Esta chave simétrica será criptografada com um algoritmo de chave assimétrico, possibilitando que apenas o destinatário, detentor da chave privada, possa obter a chave simétrica para descriptografar a mensagem com o algoritmo de chave simétrica. Assim, o arquivo a ser enviado ao e-Financeira conterá uma mensagem criptografada simetricamente e sua chave criptografada assimetricamente com a chave pública do Certificado ICP-Brasil do e-Financeira.

Ao recepcionar o arquivo criptografado, o e-Financeira realizará os procedimentos para descriptografia e obterá o arquivo XML original (anexado na mensagem). Com este XML, o e-Financeira realizará as verificações necessárias e executará os processos do evento solicitado. Por fim, será gerado o Recibo do Evento que será assinado pelo e-Financeira e enviado para a Instituição Financeira declarante. O arquivo de Recibo de Evento não será criptografado, mas sim assinado digitalmente.

4.1.2. Fluxo para Geração e Envio de Lotes Criptografados

CLIENTE (Instituição Financeira)			**SERVIDOR (e-Financeira)**
1	Definir uma chave de Criptografia AES	*	
2	Criptografar o arquivo XML a ser enviado ao e-Financeira (utilizando a Chave de Criptografia, definida no item 1).	*	
3	Criptografar a Chave de Criptografia, definida no item 1, com a Chave Pública do Certificado Digital ICP Brasil do Servidor e-Financeira.	*	
4	Gerar um novo arquivo XML do e-Financeira, contendo: • Identificação de Evento de envio de Dados e-Financeira em modo Criptografado. • Identificação (thumbprint do certificado do servidor da e-Financeira) • Chave de Criptografia (gerada no item 3). • Mensagem criptografada (gerada no ítem2)	*	
5	Estabelecer túnel TLS com o Web Service do e-Financeira.	<-->	Estabelecer túnel TLS com o Web Service Cliente da Instituição Financeira.
6	Enviar ao servidor e-Financeira, o arquivo XML (gerado no item 4).	-->	

7		*	Verificar a estrutura do XML.
8		*	Descriptografar a Chave Simétrica, com a Chave Privada do Certificado do e-Financeira.
9		*	Com a Chave Simétrica (obtida no item 8), decriptografar a Mensagem (arquivo xml criptografado).
10		*	Processar o arquivo XML (obtido na descriptografia da mensagem) e realizar as validações do e-Financeira.
11		*	Gerar o Recibo do(s) Evento(s).
12		*	Assinar o recibo do evento.
13		<--	Enviar Lote Retorno ao Cliente.

4.1.3. Passos geração Chave e Lote criptografado

1. Gerar uma chave/vetor inicialização AES-CBC 128 randomicamente.

2. Encriptar o arquivo xml de lote original com a chave AES-CBC 128 gerada.

3. Encriptar a chave AES-CBC 128 gerada no item 2, com a chave pública do certificado e-Financeira gerado exclusivamente para este fim, utilizando o algoritmo RSA com chave de 2048 bits. (Este certificado está disponível no site do Portal SPED na sessão da e-Financeira para download)

4. Gerar o arquivo XML conforme schema de envio de arquivo de lote criptografado

4.1.4. Padrões criptografia Lotes e-Financeira

- Algoritmo Assimétrico: RSA - 2048 Bits
- Padding para Criptografia Simétrica: PKCS#7
- Padding para Criptografia Assimétrica: PKCS#1 V1.5
- Algoritmo de Criptografia Simétrico: AES - 128 Bits – CBC
- Vetor de Inicialização: Concatenar o Vetor de Inicialização, em Binário. Ao final da Chave Criptográfica (também em binário) encriptar e depois proceder a conversão para Base64.
- Codificação para escrita do XML: Base64

4.1.5. Mensagens específicas para inconsistência em Lote Criptografado

MS0041 - Erro na estrutura do xml do lote criptografado
Ocorre quando há erro na validação do xml recebido com o Schema definido

MS0042 - Não foi possível descriptografar a chave com o identificador (thumbprint) do certificado chave pública do servidor da e-Financeira informado
Ocorre quando foi passado um identificado do certificado (thumbprint) que não é referente ao certificado do servidor da e-Financeira.

MS0043 - Não foi possível descriptografar o lote de eventos utilizando a chave informada
Ocorre quando o servidor da e-Financeira não consegue descriptografar o lote com a chave que foi informada.

4.2. Compactação de Lotes

A solução técnica para a recepção de lotes compactados pelo sistema e-Financeira visa permitir uma melhora de performance na transmissão dos arquivos. O uso dessa solução é opcional por parte das entidades obrigadas à e-Financeira, no entanto recomenda-se sua utilização devido ao ganho potencial de performance nessa transmissão.

O modelo da compactação foi proposto segundo as premissas abaixo:

- Utilizar o formato Gzip para compressão, devido a ser um padrão aberto e público;
- Possibilitar uma troca de arquivos com um fluxo mais ágil, pois a compactação permitirá um menor fluxo de dados transitando na rede;
- Foi priorizada uma rápida implementação com segurança e robustez.

4.2.1. Modelo de Compactação Gzip

O modelo utiliza Gzip para compactar os arquivos a serem enviados pelas Instituições Financeiras. O Gzip é um mecanismo de compressão público e livre, sendo uma tecnologia aceita no mercado profissional e acadêmico.

4.2.2. Processo para Geração de um Lote Criptografado e Compactado Gzip

1. Criar o xml de Lote conforme schema envio lotes (modo assíncrono);
2. Compactar o xml utilizando o padrão Gzip;
3. Com o array de bytes do lote compactado, deve ser feito o processo de criptografia padrão da e-Financeira;

5. Transmissão de Lotes - Modo Assíncrono

A transmissão de Lotes no modo assíncrono é baseada em APIs REST. Para cada Lote recebido a e-Financeira retornará um número de protocolo para consulta posterior ao resultado de seu processamento.

São disponibilizadas APIs e endpoints para transmissão do lote e também posterior consulta do resultado do processamento assíncrono do Lote.

O meio físico de comunicação utilizado será a internet, com o uso do protocolo HTTPS, com autenticação mútua, que além de garantir um duto de comunicação seguro na internet, permite a identificação do servidor e do cliente através de certificados digitais.

A quantidade máxima de eventos por lote assíncrono será de 50 eventos, conforme definido no schema xsd.

5.1. API REST para Transmissão de Lote

Endereços	*(ATENÇÃO : Ambientes disponíveis somente após a data da implantação prevista no Portal do SPED)* **Ambiente de Testes - Produção Restrita:** https://pre-efinanceira.receita.fazenda.gov.br/recepcao/lotes/cripto https://pre-efinanceira.receita.fazenda.gov.br/recepcao/lotes/criptoGzip **Produção:** https://efinanceira.receita.fazenda.gov.br/recepcao/lotes/cripto https://efinanceira.receita.fazenda.gov.br/recepcao/lotes/criptoGzip
Método HTTP	POST
Body / Media Type	application/xml
Requer Certificado?	Sim
Documentação Swagger	https://pre-efinanceira.receita.fazenda.gov.br/recepcao/swagger/index.html *(Será disponibilizada somente no ambiente de testes - produção restrita)*

5.2. Processo de Transmissão de Lote no modo Assíncrono

- Via endpoint **/lotes/cripto**

a. Gerar um XML de Lote modo Assíncrono (schema envioLoteEventosAssincrono-v1_0_0.xsd)
b. Gerar um XML de Lote Criptografado (schema envioLoteCriptografado-v1_2_0.xsd) cuja tag lote contem o conteudo da criptografia do lote gerado no passo a).
c. Fazer a requisição POST no endpoint passando no body o XML gerado no passo b)

- Via endpoint **/lotes/criptoGzip**
    a. Gerar um XML de Lote modo Assíncrono (schema envioLoteEventosAssincrono-v1_0_0.xsd)
    b. Compactar o conteúdo do XML gerado no passo a) com Gzip
    c. Gerar um XML de Lote Criptografado (schema envioLoteCriptografado-v1_2_0.xsd) cuja tag lote contem o conteudo da criptografia do lote gerado no passo b).
    d. Fazer a requisição POST no endpoint passando no body o XML gerado no passo c)

5.3. Códigos retorno HTTP previstos para a API de Recepção

HTTP 201	Lote recebido com sucesso pela API da e-Financeira. No body é retornado o XML contendo o protocolo do lote recebido.
HTTP 405	Método HTTP incorreto. Use o método POST para enviar lotes.
HTTP 413	Tamanho da mensagem é maior que o permitido. Tamanho máximo: 60 MB
HTTP 415	Media type não é 'application/xml', ou o conteúdo do body informado não é um XML.
HTTP 422	Lote não foi recebido pois possui inconsistências. No body é retornado o XML com as ocorrências a serem resolvidas pela instituição declarante.
HTTP 429	Excesso de conexões em sequência. Aguarde alguns minutos e tente novamente.
HTTP 495,496	Certificado não aceito na conexão à API. Verifique se o certificado está expirado ou revogado.
HTTP 500	Erro interno na recepção da escrituração e-Financeira. Aguarde alguns minutos e tente enviar o lote novamente.
HTTP 503	Serviço indisponível momentaneamente. Aguarde alguns minutos e tente novamente.

5.4. Retorno Recepção XML Lote modo Assíncrono e tag cdResposta

O XML no *body* de retorno seguirá o schema retornoLoteEventosAssincrono-v1_0_0.xsd, disponibilizado no Portal do SPED.

Valores possíveis para a tag *cdResposta* :

- 1 : Indica que o lote está em processamento pela e-Financeira.
- 7 : Lote não foi recebido, pois possui inconsistências a serem corrigidas.
- 9 : Erro interno na e-Financeira. No body de retorno é retornado o código para acionamento via fale conosco, caso o problema persista.

5.5. API REST para Consulta do Processamento de Lote

Para obter o resultado do processamento de um Lote no modo Assíncrono, o sistema cliente efetuar a chamada à API REST abaixo :

Endereços	*(ATENÇÃO : Ambientes disponíveis somente após a data da implantação prevista no Portal do SPED)* **<u>Ambiente de Testes - Produção Restrita:</u>**

	https://pre-efinanceira.receita.fazenda.gov.br/consulta/lotes/***{numeroProtocolo}*** **Produção:** https://efinanceira.receita.fazenda.gov.br/consulta/lotes/***{numeroProtocolo}***
Método HTTP	GET
Requer Certificado?	Sim
Parâmetro/uri	numeroProtocolo
Schema Retorno	retornoLoteEventosAssincrono-v1_0_0.xsd
Documentação Swagger	https://pre-efinanceira.receita.fazenda.gov.br/consulta/swagger/index.html (Será disponibilizada somente no ambiente de testes - produção restrita)

5.6. Processo de Consulta do Processamento de Lote no modo Assíncrono

Atenção : Devido a natureza assíncrona do processamento. Após obter o número de protocolo do Lote, recomendamos que o sistema cliente aguarde até 30 segundos para iniciar as consultas ao protocolo recebido.

Para realizar a consulta, o sistema cliente deve:

- Utilizar certificado digital na conexão HTTPS à API.
- Efetuar um HTTP GET no *endpoint* passando o 'numeroProtocolo' na *uri*.
- A e-Financeira retornará o XML de retorno do processamento do Lote.

5.7. Códigos retorno HTTP previstos para a API de Consulta de Lote no modo Assíncrono

HTTP 200	Lote encontrado. No body é retornado o XML com o resultado dos eventos do lote processados e seus respectivos recibos. Caso o lote ainda não tenha sido processado, será retornado o XML de lote informando que ainda está em andamento.
HTTP 404	Lote não encontrado com o protocolo informado. No body é retornado o XML contendo a informação de lote não encontrado.
HTTP 405	Método HTTP incorreto. Use o método GET para efetuar consultas.
HTTP 422	A consulta realizada possui inconsistências. No body é retornado o XML com as ocorrências a serem resolvidas pelo sistema consultante.

HTTP 429	Excesso de consultas/conexões em sequência. Aguarde alguns minutos e tente novamente.
HTTP 495, 496	Certificado não aceito na conexão a API. Verifique se o certificado está expirado ou revogado.
HTTP 500	Erro interno na e-Financeira. Aguarde alguns minutos e tente realizar a consulta novamente.
HTTP 503	Serviço indisponível momentaneamente. Aguarde alguns minutos e tente novamente.

5.8. Retorno Consulta de Lote no modo Assíncrono e tag cdResposta

O XML no *body* de retorno seguirá o schema retornoLoteEventosAssincrono-v1_0_0.xsd, disponibilizado no Portal do SPED.

Valores possíveis para a tag cdResposta:

- 1 : Indica que o lote ainda está em processamento pela e-Financeira.
- 2 : O lote foi processado. Todos os eventos foram processados com sucesso.
- 3 : O lote foi processado. Possui um ou mais eventos com ocorrências.
- 4: A própria consulta possui ocorrências e a busca do lote não foi executada. Verificar ocorrências no XML de retorno.
- 5 : A consulta foi executada, porém o lote não foi encontrado.
- 9 : Erro interno na e-Financeira.

5.9. Uso abusivo de Consultas / rate limiting

O excesso de tentativas de consultas em sequência poderá ser considerado uso abusivo do sistema, e a API responderá com código HTTP 429 para esses casos. O usuário deverá então aguardar alguns minutos para efetuar consultas novamente.

6. Transmissão Lotes – Ambiente de Testes (Produção Restrita)

O ambiente de testes (produção restrita) ficará disponível indefinidamente, até posição contrária da Receita Federal do Brasil, para qualquer entidade obrigada pela IN RFB nº 1.571/2015 enviar arquivos de testes para verificar o funcionamento de seus sistemas.

Este ambiente não deve ser usado para testes de volumetria. O ambiente está dimensionado e deve ser usado apenas para testar itens como: estrutura dos XMLs, assinatura dos eventos, transmissão dos dados, validação do conteúdo dos arquivos, entre outras questões relativas ao negócio.

Haverá uma limitação de 1000 eventos de cada tipo de movimento (operação financeira, previdência privada, rerct) por declarante. Uma vez atingida essa quantidade, o declarante deverá utilizar a funcionalidade de limpeza dos dados conforme o item *"Endpoint para Limpeza de dados no Ambiente de Testes (Produção Restrita)"* deste manual, e depois continuar a enviar eventos normalmente. Quando atingir novamente o limite de 1000, deverá novamente limpar os dados, e assim sucessivamente.

Este ambiente não conta com apoio técnico, tanto via e-mail ou telefone, por parte da Receita Federal ou Serpro.

Os dados do ambiente de produção restrita serão excluídos a cada fim de semestre, confome informação do item *"Ambiente de Testes - Produção Restrita : Exclusão automática dos dados a cada fim de semestre."* deste manual.

7. Consulta das informações enviadas em Eventos

Os serviços de consultas das informações enviadas para a e-Financeira foram projetados para receberem um ou mais parâmetros de entrada, e retornarem mensagens no padrão XML.

Em situações de contingência, as consultas também poderão ser efetuadas por meio do Portal do SPED, no seguinte endereço : http://sped.rfb.gov.br/pagina/show/1779

7.1.1. API REST para Consultas de dados enviados em Eventos

O modelo de uso de APIs REST para consultas aos dados enviados em Eventos será em modo assíncrono.

Processo da Consulta :

1 - A aplicação cliente efetua uma requisição POST ao endpoint do tipo de consulta desejada, passando os devidos parâmetros no body, com content-type application/x-www-form-urlencoded.

2 - A API da e-Financeira retorna um XML conforme schema retornoSolicitacaoConsultaAssincrona-v1_0_0.xsd;

3 - No XML retornado, a aplicação cliente obtém o número do protocolo da solicitação de consulta;

4 - Com o número de protocolo, a aplicação cliente efetua uma requisiçao GET ao endpoint da consulta com o número do protocolo, e obtém o xml de resultado da consulta.

URL Base	*(ATENÇÃO : Ambientes disponíveis somente após a data da implantação prevista no Portal do SPED)* **Ambiente de Testes - Produção Restrita:** https://pre-efinanceira.receita.fazenda.gov.br/consulta **Produção:** https://efinanceira.receita.fazenda.gov.br/consulta
Requer Certificado ?	Sim. O certificado deve atender a uma das seguintes exigências: • Ser o responsável pela informação. • Ser procurador do responsável pela informação

Endpoints para solicitação de consultas **(POST)**	**<u>Consulta Informações Cadastrais</u>** **Endpoint :** https://{URL base}/**informacoes-cadastrais** **Content Type :** application/x-www-form-urlencoded **Body/Parâmetros :** cnpj={cnpj} **<u>Consulta Lista e-Financeira (módulos Mov. Financeira e Previdência Privada)</u>** **Endpoint :** https://{URL base}/**lista-efinanceira-movimento** **Content Type :** application/x-www-form-urlencoded **Body/Parâmetros :** cnpj={cnpj}&situacaoInformacao={situacaoInformacao}&dataInicio={dataInicio}&dataFim={dataFim} **<u>Consulta Informações Movimento Operação Financeira</u>** **Endpoint :** https://{URL base}/**informacoes-mov-op-fin** **Content Type :** application/x-www-form-urlencoded **Body/Parâmetros :** cnpj={cnpj}&situacaoInformacao={situacaoInformacao}&anoMesInicioVigencia={anoMesInicioVigencia}&anoMesTerminoVigencia={anoMesTerminoVigencia}tipoIdentificacao={tipoIdentificacao}&identificacao={identificacao} **<u>Consulta Informações Movimento Operação Financeira Anual</u>** **Endpoint :** https://{URL base}/**informacoes-mov-op-fin-anual** **Content Type :** application/x-www-form-urlencoded **Body/Parâmetros :** cnpj={cnpj}&situacaoInformacao={situacaoInformacao}&anoMesInicioVigencia={anoMesInicioVigencia}&anoMesTerminoVigencia={anoMesTerminoVigencia}tipoIdentificacao={tipoIdentificacao}&identificacao={identificacao} **<u>Consulta Informações Movimento Previdência Privada</u>** **Endpoint :** https://{URL base}/**informacoes-mov-pp** **Content Type :** application/x-www-form-urlencoded **Body/Parâmetros :** cnpj={cnpj}&situacaoInformacao={situacaoInformacao}&anoMesInicioVigencia={anoMesInicioVigencia}&anoMesTerminoVigencia={anoMesTerminoVigencia}tipoIdentificacao={tipoIdentificacao}&identificacao={identificacao} **<u>Consulta Informações Intermediário</u>** **Endpoint :** https://{URL base}/**informacoes-intermediario** **Content Type :** application/x-www-form-urlencoded **Body/Parâmetros :** cnpj={cnpj}&giin={GINN}&tipoNi={TipoNI}&numeroIdentificacao={NumeroIdentificacao} **<u>Consulta Informações Patrocinado</u>** **Endpoint :** https://{URL base}/**informacoes-patrocinado** **Content Type :** application/x-www-form-urlencoded **Body/Parâmetros :** cnpj={cnpj}&cnpjPatrocinado={cnpjPatrocinado}&giinPatrocinado={giinPatrocinado}
Endpoints para resultado de	**https://**{URL base}/**informacoes-cadastrais**/{numeroProtocolo}

consulta **(GET)**	**https://**{URL base}/**lista-efinanceira-movimento**/{numeroProtocolo} **https://**{URL base}/**informacoes-mov-op-fin**/{numeroProtocolo} **https://**{URL base}/**informacoes-mov-op-fin-anual**/{numeroProtocolo} **https://**{URL base}/**informacoes-mov-pp**/{numeroProtocolo} **https://**{URL base}/**informacoes-intermediario** /{numeroProtocolo} **https://**{URL base}/**informacoes-patrocinado**/{numeroProtocolo}
Schema Retorno para todos os endpoints (POST e GET)	retornoSolicitacaoConsultaAssincrona-v1_0_0.xsd *Quando a consulta retornar situação cdResposta = 3 – (Consulta Processada), a tag "xmlResultadoConsulta" do xsd acima conterá o xml com o resultado da consulta, que seguirá o xsd de retorno da consulta solicitada :* retornoConsultaInformacoesCadastrais-v1_3_0.xsd retornoConsultaListaEFinanceira-v1_2_0.xsd retornoConsultaInformacoesMovOpFin-v1_0_0.xsd retornoConsultaInformacoesMovOpFinAnual-v1_0_0.xsd retornoConsultaInformacoesMovPP-v1_0_0.xsd retornoConsultaInformacoesIntermediario-v1_2_0.xsd retornoConsultaInformacoesPatrocinado-v1_2_0.xsd
Documentação Swagger	(Será disponibilizada somente em produção restrita) https://efinanceira.receita.fazenda.gov.br/consulta/swagger/index.html

7.2. Parâmetros das Consultas

Consulta Informações Cadastrais			
Parâmetros			
	Tamanho	**Obrigatório**	**Valores Válidos**
cnpj (CNPJ da empresa declarante)	014	S	CNPJ Válido

Consulta Lista de e-Financeira (módulos Mov. Financeira e Previdência Privada)			
Parâmetros			
	Tamanho	**Obrigatório**	**Valores Válidos**
cnpj (CNPJ da empresa declarante)	014	S	CNPJ Válido
situacaoInformacao (Situação da Informação)	001	S	0 – Todas 1 – Em Andamento 2 – Ativa 3 - Retificada 4 - Excluída
dataInicio (Data de início da solicitação)		S	Formato DD/MM/AAAA
dataFim (Data de fim da solicitação)		S	Formato DD/MM/AAAA

Consulta Informações de Movimento Operação Financeira			
Parâmetros			
	Tamanho	**Obrigatório**	**Valores Válidos**
cnpj (CNPJ da empresa declarante)	014	S	CNPJ Válido
situacaoInformacao (Situação da Informação)	001	S	0 – Todas 1 – Ativo 2 - Retificado 3 - Excluído
anoMesInicioVigencia (Ano/Mês inicial das informações)	-	S	Formato AAAAMM
anoMesTerminoVigencia (Ano/Mês final das informações)	-	S	Formato AAAAMM
tipoIdentificacao (Tipo de Identificação do Declarado)	001	S	1=CPF 2=CNPJ 3=NIF Pessoa Física (Número de Identificação Fiscal Pessoa Física) 4=NIF Pessoa Jurídica (Número de Identificação Fiscal Pessoa Jurídica) 5=Passaporte 6=Número do PIS 7=Identidade Mercosul 99=Sem NI
identificacao (Número de Identificação)	014	S	Valor conforme tipo de Identificação do declarado.

Consulta Informações de Movimento Operação Financeira Anual

Parâmetros

	Tamanho	Obrigatório	Valores Válidos
cnpj (CNPJ da empresa declarante)	014	S	CNPJ Válido
situacaoInformacao (Situação da Informação)	001	S	0 – Todas 1 – Ativo 2 - Retificado 3 - Excluído
anoMesInicioVigencia (Ano/Mês inicial das informações)	-	S	Formato AAAAMM
anoMesTerminoVigencia (Ano/Mês final das informações)	-	S	Formato AAAAMM
tipoIdentificacao (Tipo de Identificação do Declarado)	001	S	1=CPF 2=CNPJ 3=NIF Pessoa Física (Número de Identificação Fiscal Pessoa Física) 4=NIF Pessoa Jurídica (Número de Identificação Fiscal Pessoa Jurídica) 5=Passaporte 6=Número do PIS 7=Identidade Mercosul 99=Sem NI
identificacao (Número de Identificação)	014	S	Valor conforme tipo de Identificação do declarado.

Consulta Informações de Movimento Previdência Privada

Parâmetros

	Tamanho	Obrigatório	Valores Válidos
cnpj (CNPJ da empresa declarante)	014	S	CNPJ Válido
situacaoInformacao (Situação da Informação)	001	S	0 – Todas 1 – Ativo 2 - Retificado 3 - Excluído
anoMesInicioVigencia (Ano/Mês inicial das informações)	-	S	Formato AAAAMM
anoMesTerminoVigencia (Ano/Mês final das informações)	-	S	Formato AAAAMM
tipoIdentificacao (Tipo de Identificação do Declarado)	001	S	1=CPF 2=CNPJ 3=NIF Pessoa Física (Número de Identificação Fiscal Pessoa Física) 4=NIF Pessoa Jurídica (Número de Identificação Fiscal Pessoa Jurídica) 5=Passaporte 6=Número do PIS 7=Identidade Mercosul 99=Sem NI
identificacao (Número de Identificação)	014	S	Valor conforme tipo de Identificação do declarado.

Consulta Informações do Cadastro de Intermediário			
Parâmetros			
	Tamanho	**Obrigatório**	**Valores Válidos**
cnpj (CNPJ da empresa declarante)	014	S	CNPJ Válido
giin (GIIN do intermediário)	019	N	GIIN do intermediário
tipoNi (Identificação do Intermediário - Tipo NI)	001	N	1=CPF 2=CNPJ 3=NIF Pessoa Física (Número de Identificação Fiscal Pessoa Física) 4=NIF Pessoa Jurídica (Número de Identificação Fiscal Pessoa Jurídica)
numeroIdentificacao (Identificação do Intermediário - Número do NI)	025	N	Valor conforme tipo de Identificação do declarado.

Consulta Informações do Cadastro de Patrocinado			
Parâmetros			
	Tamanho	**Obrigatório**	**Valores Válidos**
cnpj (CNPJ da empresa declarante)	014	S	CNPJ Válido
cnpjPatrocinado (CNPJ do patrocinado)	014	N	CNPJ Válido
giinPatrocinado (GIIN do patrocinado)	019	N	GIIN do Patrocinado

7.3. Retorno solicitação consulta e tag cdResposta

O XML no body de retorno seguirá o schema retornoSolicitacaoConsultaAssincrona-v1_0_0.xsd, disponibilizado no Portal do SPED.

Valores possíveis para a tag cdResposta :

- 1 : Consulta válida, e a consulta será processada de forma assíncrona. No body é retornado o xml com o protocolo informado na tag “protocoloConsulta”, a ser usado para obter o resultado do processamento da consulta.
- 2 : Consulta inválida. Verificar ocorrências no xml de retorno.
- 3 : Consulta processada. No body é retornado o xml com o resultado da solicitação.
- 9 : Erro interno na e-Financeira. No body de retorno é retornado o código para acionamento via fale conosco, caso o problema persista.

7.4. Códigos retorno HTTP previstos para a API de Consulta

HTTP 200	Solicitação de Consulta existente. No body é retornado o XML com o resultado da consulta. Caso a consulta ainda não tenha sido processada, será retornado o XML conforme retornoSolicitacaoConsultaAssincrona-v1_0_0.xsd, indicando que a consulta ainda está em processamento e seu devido número de protocolo.
HTTP 404	Solicitação de Consulta não encontrada com o protocolo informado.
HTTP 405	Método HTTP incorreto. Para solicitar consultas use o método POST, e para obter o resultado use o método GET.
HTTP 422	A consulta realizada possui inconsistências. No body é retornado o XML conforme retornoSolicitacaoConsultaAssincrona-v1_0_0.xsd contendo as ocorrências a serem resolvidas pelo sistema consultante.
HTTP 429	Excesso de consultas/conexões em sequência. Aguarde alguns minutos e tente novamente.
HTTP 495, 496	Certificado não aceito na conexão a API. Verifique se o certificado está expirado ou revogado.
HTTP 500	Erro interno na e-Financeira. Aguarde alguns minutos e tente realizar a consulta novamente.
HTTP 503	Serviço indisponível momentaneamente. Aguarde alguns minutos e tente novamente.

8. Endpoint para Limpeza de dados no Ambiente de Testes (Produção Restrita)

O que é	Endpoint disponibilizado **exclusivamente** no Ambiente de Testes (Produção Restrita) para que o declarante possa excluir os seus dados de teste sob demanda.
Como usar	A chamada e execução da limpeza será realizada de forma síncrona. O sistema acionador deve efetuar a requisição com o método HTTP DELETE e aguardar o retorno. Caso a limpeza seja executada com sucesso, será retornado HTTP 200. Mensagens de validação retornadas pelo endpoint serão devolvidas como texto no body. Todas as solicitações de limpeza serão registradas no ambiente da e-Financeira.
URL	https://pre-efinanceira.receita.fazenda.gov.br/recepcao/limpezaDadosTesteProducaoRestrita?cnpjDeclarante=***[cnpj]***

	Onde ***[cnpj]*** é o CNPJ do declarante para o qual os dados devem ser excluídos. O valor do ***[cnpj]*** deve ser informado contendo ***somente números*** e ***sem formatação.***
Metódo HTTP	**DELETE**
Requer Certificado ?	Sim. O certificado deve atender a uma das seguintes exigências: • Ser o responsável pelo cnpjDeclarante informado. • Ser procurador do cnpjDeclarante informado.
Retornos HTTP esperados	200 - Limpeza efetuada com sucesso. 400 - Parametro cnpjDeclarante não informado ou inválido. 401 - O certificado usado na conexão é inválido ou não possui permissao para limpar dados do cnpjDeclarante informado. 404 – URL informada incorretamente. Serviço não encontrado. 405 - Não foi utilizado o método HTTP DELETE na chamada ao endpoint. 495, 496 – Não foi utilizado certificado válido na chamada ao endpoint. 500 - Erro interno na e-Financeira. Retornada mensagem com o código de erro no body de retorno.

9. Recomendações e Boas Práticas

O objetivo desta seção é orientar os usuários a utilizarem os serviços da e-Financeira seguindo boas práticas, facilitando a integração com o sistema e colaborando para um ambiente mais saudável para todos.

9.1. Otimizar a montagem do arquivo

Evitar incluir tags de campo com conteúdo zero (para campos tipo numérico) ou vazio (para campos tipo caractere) na geração do arquivo XML, exceto para os campos identificados como obrigatórios no modelo. Para reduzir o tamanho final do arquivo XML a ser transportado, alguns cuidados de programação deverão ser assumidos:

- não incluir "zeros não significativos" para campos numéricos, exceto quando o campo possuir um universo definido de valores válidos;
- não incluir "espaços" no início ou no final de campos numéricos e alfanuméricos;
- não incluir comentários no arquivo XML;
- não incluir anotação e documentação no arquivo XML (tag annotation e tag documentation);
- não incluir caracteres de formatação.

9.2. Eventos de movimento com muitas contas

Em caso de eventos de movimento com mais de mil contas, é recomendado enviá-lo em separado num lote. Ou seja, gere um lote somente com esse evento.

9.3. Evitar consultas repetidas em excesso

Evitar excesso de requisições em sequência nas APIs de consultas, pois poderá ser considerado uso abusivo do sistema. Será retornado código HTTP 429 para esses casos, e o usuário deverá então aguardar alguns minutos para poder efetuar consultas novamente.

9.4. Aguardar para iniciar a consulta ao protocolo de um Lote no modo Assíncrono

Após obter o número de protocolo de um Lote no modo Assíncrono, recomenda-se aguardar no mínimo 30 segundos para iniciar a consulta ao protocolo.

9.5. Enviar evento de 'Fechamento' em Lote separado, e somente após finalizar todo o envio de eventos de Movimento

Enviar o evento de Fechamento em Lote separado.

Enviar o Lote contendo o evento de Fechamento somente após o envio de todos os eventos de Movimento e obtenção de seus respectivos recibos.

9.6. Ambiente de Testes - Produção Restrita : Exclusão automática dos dados a cada fim de semestre

A cada fim de prazo de entrega (1º de março e 1º de setembro), todos os dados do ambiente de produção restrita serão excluídos, ou seja, as informações do ambiente serão zeradas.