Operador Nacional | Registro Civil do Brasil

E-PROTOCOLO 2.0 - INTEGRAÇÃO COM UNIDADE INTERLIGADA E E-ÓBITO

Sumário

Sumário **2**
Apresentação 3
Para quem é este documento 3
O que este documento não cobre 3
Visão geral do serviço 3
Requisitos iniciais 4
Credenciais de acesso 4
Checklist de requisitos 5
Ambientes e entrada em produção 5
Fluxo de integração 6
Autenticação e tokens 8
Token do IdRC para o cumprimento 8
Eventos e ações esperadas 9
Conteúdo adicional por status 11
Como receber e usar os arquivos estruturados 11
Como identificar e recuperar o arquivo 12
Como usar o arquivo para gerar o registro 12
Fluxo: Unidade Interligada (nascimento) 13
Fluxo: e-Óbito (óbito) 14
Estratégia de consumo 14
Rotas do serviço 15
O que o cumprimento exige 16
Responsabilidades 16
Segurança e proteção de dados 17
Índice de regras 17
Glossário 18

Apresentação

Este documento descreve o contexto, o fluxo e os requisitos iniciais para integrar um sistema de cartório ao **Serviço de Pendências do e-Protocolo 2.0**. Ele explica o que precisa estar pronto antes de começar, como as rotas se encadeiam e quais cuidados garantem que nenhuma pendência se perca.

Para quem é este documento

Público	O que buscar aqui
Oficial e gestão do cartório	Requisitos iniciais, geração das credenciais, responsabilidades e proteção de dados.
Equipe de TI do cartório	Visão geral, ambientes, fluxo de integração e estratégia de consumo.
Empresa integradora (software do cartório)	Fluxo de integração, eventos e ações esperadas, papel de cada rota e boas práticas.

O que este documento não cobre

Os detalhes técnicos de cada rota (parâmetros, campos, tipos, valores possíveis e exemplos de requisição e resposta) estão na referência técnica da API: https://eventosh.registrocivil.org.br/reference. Em caso de divergência, a referência técnica prevalece.

Visão geral do serviço

O Serviço de Pendências permite que o sistema do cartório saiba, sem acesso manual ao e-Protocolo, quando um protocolo exige sua ação. Com ele, o sistema consulta os dados e arquivos do protocolo e registra o cumprimento diretamente pela API.

A integração funciona por **consulta periódica** (**polling**): é o sistema do cartório que busca as notificações. O e-Protocolo não envia chamadas para o cartório.

As rotas ficam em dois serviços, e um único token de acesso vale para ambos:

Serviço	Homologação	Produção
Eventos: autenticação e notificações	`https://eventosh.registrocivil.org.br`	`https://eventos.registrocivil.org.br`
Protocolo: consulta, arquivos e cumprimento	`https://protocoloh.registrocivil.org.br`	`https://protocolo.registrocivil.org.br`

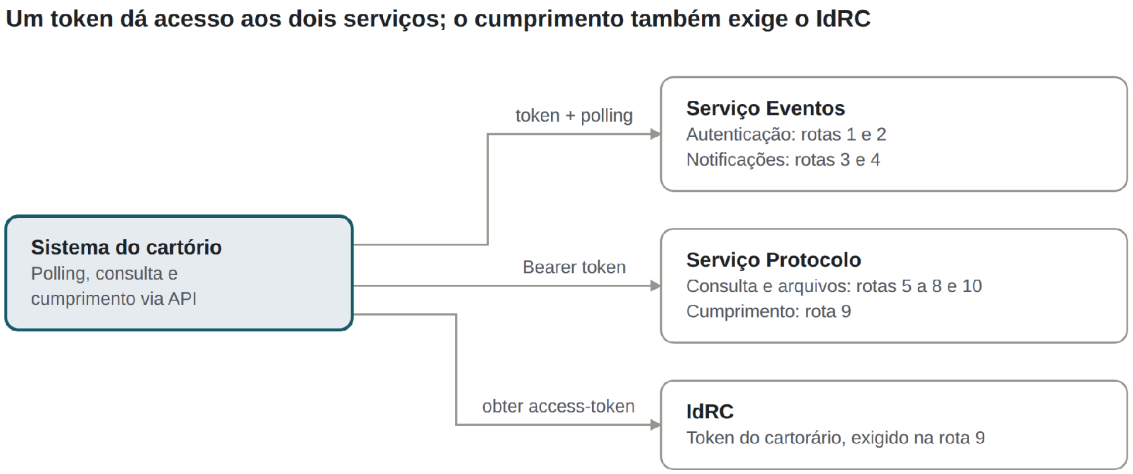


Figura 1 – Arquitetura da integração: sistema do cartório, serviços Eventos e Protocolo e IdRC

Requisitos iniciais

Antes da primeira chamada, os itens abaixo precisam estar resolvidos. Parte deles depende do cartório e parte da equipe que fará a integração.

Credenciais de acesso

As credenciais (usuário e senha) são geradas pelo **oficial do cartório**, no botão "Serviço de pendências" da plataforma do e-Protocolo (https://protocolo.registrocivil.org.br).

- É permitida **uma credencial por cartório**.
- Por segurança, as credenciais são exibidas **uma única vez**, no momento da geração. Devem ser repassadas à equipe de integração por canal seguro e guardadas em cofre de senhas.

- Em caso de perda ou suspeita de vazamento: Em caso de perda ou suspeita de vazamento, entrar em contato com a equipe de suporte: https://serp.movidesk.com/form/11089/

Checklist de requisitos

Requisito	Responsável	Como atender
Credenciais de produção geradas	Oficial do cartório	Botão "Serviço de pendências" no e-Protocolo.
Credenciais de homologação	Oficial do cartório	Botão "Serviço de pendências" no e-Protocolo.
Cartorários com acesso ao IdRC	Cartório	O token do IdRC é exigido no cumprimento (cabeçalho `access-token`).
Client IdRC da plataforma	Integrador	Solicitar em https://integracao.idrc.registrocivil.org.br/solicitacao-novo-client. Necessário para obter o token do cartorário.
Dados do responsável pelo cumprimento	Cartório	CPF, nome, e-mail do cartorário e CNS do cartório.
Saída HTTPS liberada	TI / integrador	Domínios dos serviços Eventos e Protocolo, nos dois ambientes.
Armazenamento seguro de credenciais e tokens	Integrador	Fora do código-fonte, em cofre ou variável protegida.
Rotina agendada de polling	Integrador	Ver "Estratégia de consumo".
Persistência das notificações recebidas	Integrador	Cada notificação é entregue uma única vez.
Rotina de reconciliação	Integrador	Consulta periódica do histórico de notificações.

Ambientes e entrada em produção

Toda integração deve ser construída e validada primeiro em **homologação**. Antes de usar as URLs de produção, recomenda-se validar ao menos os cenários abaixo.

Cenário de teste	Resultado esperado
Autenticação com credenciais válidas e inválidas	Token obtido; credencial inválida tratada sem travar a rotina.
Token expirado durante o ciclo	Nova autenticação automática e repetição da chamada.
Lote com várias notificações	Todas gravadas antes do processamento; nenhuma perdida.
Consulta de protocolo, anexos e arquivo estruturado	Dados e arquivos obtidos pelo hash da notificação.
Cumprimento com certidão eletrônica e física	Protocolo cumprido e evento de conclusão recebido.
Erros 404, 422 e 429	Tratados com registro em log e nova tentativa quando aplicável.
Reconciliação pelo histórico	Notificações já processadas não são tratadas de novo.

Suporte técnico durante a homologação: https://serp.movidesk.com/form/11089/

Fluxo de integração

O ciclo de trabalho do sistema integrador se repete a cada execução do polling. O **hash** recebido na notificação é a chave que liga as rotas dos dois serviços: todas as consultas e o cumprimento no serviço Protocolo usam esse valor.

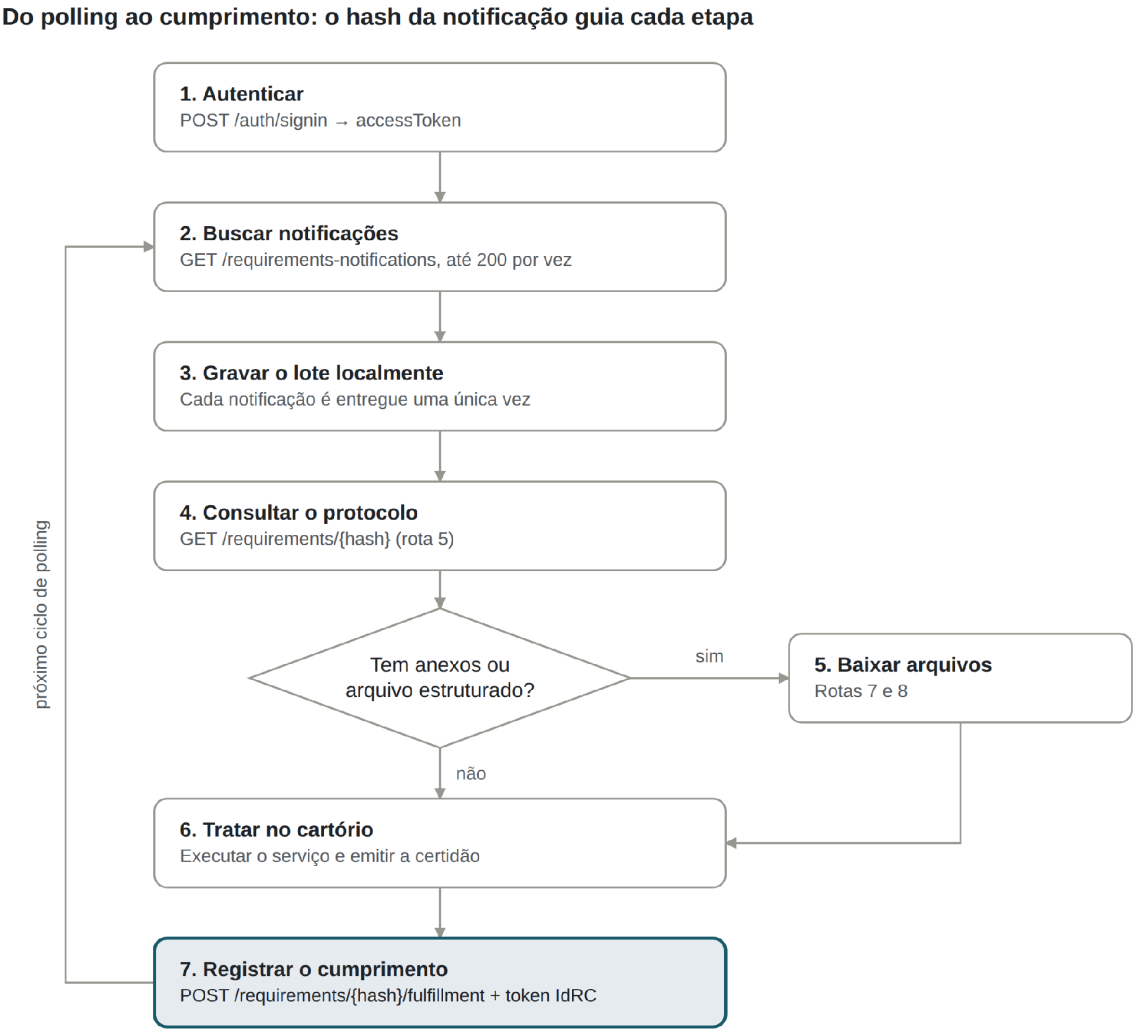


Figura 2 – Fluxo de integração, da autenticação ao cumprimento

Etapa	O que fazer	Rota
1. Autenticar	Obter o token com as credenciais do cartório. Repetir sempre que uma chamada retornar 401.	1
2. Buscar notificações	Consultar as notificações não lidas. Se ainda houver pendentes, chamar novamente.	3
3. Gravar o lote	Persistir as notificações antes de processar; elas não serão entregues de novo.	—
4. Consultar o protocolo	Obter os dados atualizados pelo hash recebido.	5
5. Baixar arquivos	Quando houver anexos ou arquivo estruturado.	7 e 8
6. Tratar no cartório	Executar o serviço no sistema do cartório e emitir a certidão.	—

Etapa	O que fazer	Rota
7. Registrar o cumprimento	Informar a certidão e o responsável, com o token do IdRC.	9

Autenticação e tokens

O token de acesso é obtido na rota de autenticação e enviado em todas as demais rotas, nos dois serviços, no cabeçalho:

HTTP — Cabeçalho de autorização

```
Authorization: Bearer SEU_TOKEN
```

A validade do token é de 10 minutos. Na prática, o sistema deve tratar qualquer resposta 401 autenticando de novo e repetindo a chamada. A rota de validação do token pode ser usada antes de um lote de chamadas.

A rota de cumprimento exige, além do Bearer token, o token do **IdRC** do cartorário responsável, enviado no cabeçalho `access-token`.

Token do IdRC para o cumprimento

O token do IdRC identifica o usuário (cartorário) que realiza o cumprimento. Ele é gerado após o próprio usuário se autenticar e autorizar o acesso no IdRC, e está vinculado à sessão desse usuário no IdRC.

Para que a sua plataforma ou serviço permita o fluxo de autenticação de usuários no IdRC, é necessário possuir um **client IdRC**. Para solicitar um novo client, acesse: https://integracao.idrc.registrocivil.org.br/solicitacao-novo-client.

Para saber mais sobre o fluxo de autenticação no IdRC, consulte a documentação do fluxo de autenticação do IdRC.

A obtenção segue o fluxo de autorização por código:

Passo	O que acontece
1	A plataforma direciona o cartorário para o IdRC, onde ele se autentica e autoriza o acesso.
2	O IdRC retorna para a plataforma pela URL informada em `redirect_uri`, enviando um código de autorização (`code`).
3	A plataforma envia o `code` ao endpoint de token do IdRC e recebe os tokens do usuário.

Passo	O que acontece
4	O `access_token` é enviado no cabeçalho `access-token` da rota de cumprimento.

O endpoint de token devolve três tokens:

Token	Para que serve	Validade
`id_token`	Representa a sessão do usuário e contém seus dados.	5 minutos
`access_token`	Token do usuário, exigido no cumprimento (cabeçalho `access-token`).	5 minutos
`refresh_token`	Renova a sessão e permite obter um novo `access_token` sem nova autenticação.	8 horas

O `access_token` tem validade de apenas **5 minutos**. Por isso, ele deve ser renovado imediatamente antes do cumprimento, utilizando o `refresh_token`, ou de forma recorrente, também por meio do `refresh_token`. O `refresh_token` tem validade de **8 horas** e, enquanto estiver dentro desse prazo, permite obter novos `access_token` sem que o usuário precise se autenticar novamente.

Após 5 minutos, o `access_token` é considerado expirado e não pode mais ser utilizado.

Se o `refresh_token` também estiver expirado (mais de 8 horas), a sessão é encerrada e o cartorário precisa se autenticar novamente no IdRC, informando seu CPF e senha, além de um segundo fator de autenticação.

Eventos e ações esperadas

Cada notificação informa, no campo `status`, o evento que acabou de ocorrer no protocolo. O quadro agrupa os eventos por etapa e indica a ação esperada do sistema do cartório. Alguns eventos trazem dados extras no campo `content`.

Etapa	Evento (status)	Significado	Ação esperada
Entrada	`request_received`	Requerimento recebido	Consultar o protocolo e iniciar o atendimento
Assinatura	`signature_completed`	Documento assinado pelo cidadão	Atualizar o andamento

Etapa	Evento (status)	Significado	Ação esperada
Exigência	`waiting_for_response_requirement_note`	Nota de exigência enviada	Aguardar resposta do solicitante
Exigência	`requirement_note_answered`	Nota de exigência respondida	Analisar a resposta
Exigência	`requirement_note_finished`	Nota de exigência finalizada	Retomar o atendimento
Orçamento	`send_for_budget`	Enviado para orçamento	Atualizar o andamento
Orçamento	`budget_response`	Orçamento aguardando aprovação	Aguardar decisão do solicitante
Orçamento	`waiting_approval_for_additional_services`	Serviços adicionais aguardando aprovação	Aguardar decisão do solicitante
Pagamento	`waiting_for_payment`	Aguardando pagamento	Aguardar o pagamento
Pagamento	`payment_made`	Pagamento realizado	Executar o serviço e preparar o cumprimento
Devolução	`devolved`	Protocolo devolvido	Analisar o motivo
Devolução	`accepted_devolution`	Devolução aceita	Atualizar o andamento
Devolução	`rejected_devolution`	Devolução recusada (motivo em `content`)	Analisar o motivo
Encerramento	`transferred_to_another_notary`	Transferido para outra serventia (novo protocolo em `content`)	Encerrar localmente e registrar o destino
Encerramento	`canceled`	Cancelado (motivo em `content`, quando houver)	Encerrar localmente
Encerramento	`completed`	Protocolo cumprido (link da certidão em `content`, quando eletrônica)	Confirmar a conclusão

A ordem exata das transições entre status não está formalizada. O sistema não deve depender de uma sequência fixa: deve sempre consultar o protocolo para conhecer seu estado atual.

Conteúdo adicional por status

O objeto `content` só é preenchido nos status abaixo. Nos demais, é retornado vazio.

Status	Campos em content
`requirement_note_finished`	`requirement_note_status`: "requirement_note_finished".
`rejected_devolution`	`rejection_reason`: motivo da recusa.
`canceled`	`cancellation_reason`: motivo do cancelamento. Enviado somente quando o cancelamento é feito pelo cidadão, pelo cartório ou pela nota. Em cancelamentos por API de terceiros, ferramenta de correção ou job de expiração, o motivo não é enviado.
`completed`	`certificate_link`: link da certidão gerada, em casos de emissão de certidão eletrônica.
`transferred_to_another_notary`	`new_requirement_id`, `new_requirement_hash` e `new_notary_cns`: dados do novo protocolo e da serventia de destino.

Como receber e usar os arquivos estruturados

O **arquivo estruturado** é um arquivo JSON com os dados necessários para o cartório **gerar o registro e emitir a certidão**, sem redigitar as informações. Ele acompanha os protocolos abertos pela **Unidade Interligada** (registro de nascimento, a partir de hospitais e maternidades) e pelo **e-Óbito** (registro de óbito, a partir de funerárias e IMLs).

Origem	Quem abre o protocolo	Registro	Identificação no arquivo
Unidade Interligada	Hospitais e maternidades	Nascimento	`plataformaId`: `unidade_interligada`; `tipo_registro`: `nascimento`
e-Óbito	Funerárias e IMLs	Óbito	`plataformaId`: `e-obito`; `tipo_registro`: `obito`

Como identificar e recuperar o arquivo

Na rota de detalhamento do protocolo (rota 5), o atributo `hasStructuredFile` indica se o protocolo possui arquivo estruturado:

JSON — trecho do detalhamento do protocolo

```
"hasStructuredFile": true
```

Valor	O que fazer
`true`	O protocolo possui arquivo estruturado. Recuperá-lo pela rota 8: GET `/api/v1.0/notifications-system/requirements/{hash}/structured-file`.
`false`	Não há arquivo estruturado: a rota 8 retorna 404. O registro segue pelo fluxo habitual, com base nos dados e anexos do protocolo.

Como usar o arquivo para gerar o registro

O arquivo tem duas partes: `solicitacao`, que identifica a origem e o cartório de destino, e `registro`, com os dados para a lavratura. O sistema do cartório deve:

Etapa	O que fazer
1. Identificar o tipo	Ler `plataformaId` e `tipo_registro` para direcionar o arquivo ao importador de nascimento ou de óbito.
2. Importar os dados	Preencher o registro com os blocos do arquivo (quadro abaixo), evitando a redigitação.
3. Conferir	Confrontar os dados importados com os documentos anexados ao protocolo antes da lavratura.
4. Lavrar e emitir	Gerar o registro e emitir a certidão no sistema do cartório.
5. Cumprir	Registrar o cumprimento do protocolo (rota 9).

Conteúdo	Nascimento (Unidade Interligada)	Óbito (e-Óbito)
Origem e destino	`solicitacao`	`solicitacao`
Dados do evento	`registro.dados_nascimento`: DNV e local do nascimento	`registro.dados_falecimento`: DO, data, hora, local, médicos, causas e sepultamento
Pessoa registrada	Dados da criança: nome, data e hora, sexo, naturalidade, gemelaridade	`registro.falecido`: dados pessoais, cônjuge, endereço e filiação

Conteúdo	Nascimento (Unidade Interligada)	Óbito (e-Óbito)
Filiação	Genitores, documentos, endereços e ascendentes	Dentro de `registro.falecido.filiacao`
Declarante	Dados e endereço do declarante	`registro.declarante`
Complementos	—	Filhos, documentos do falecido e indicadores (bens, testamento, eleitor etc.)

Fluxo: Unidade Interligada (nascimento)

Do envio da solicitação pelo hospital ou maternidade até a emissão da certidão no cartório:

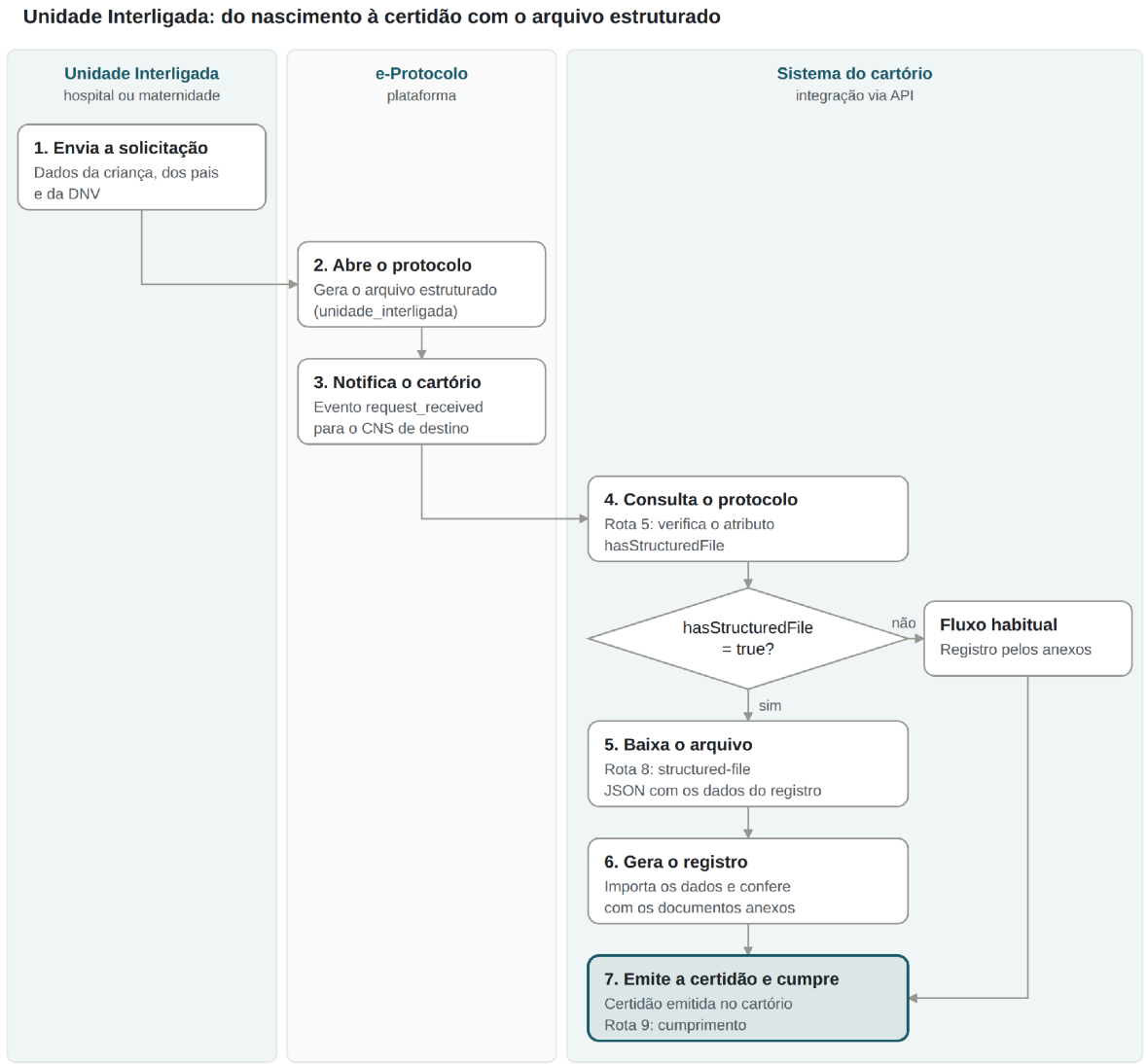


Figura 3 – Arquivo estruturado no fluxo da Unidade Interligada

Fluxo: e-Óbito (óbito)

Do envio da solicitação pela funerária ou IML até a emissão da certidão no cartório:

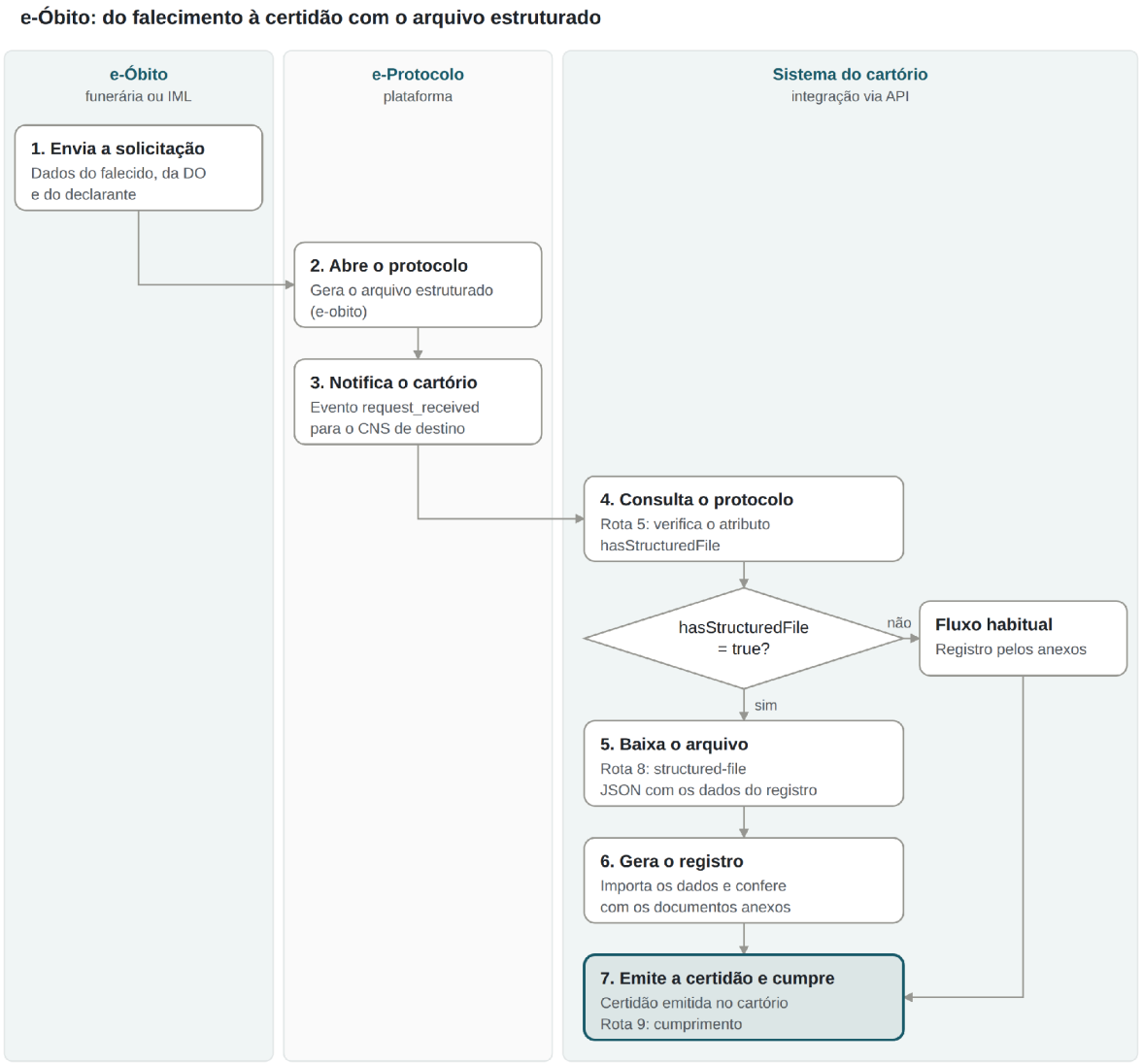


Figura 4 – Arquivo estruturado no fluxo do e-Óbito

Estratégia de consumo

A confiabilidade da integração depende mais da forma de consumir as notificações do que das rotas em si. As práticas abaixo são recomendadas.

Prática	Por que importa
Gravar antes de processar	Cada notificação é marcada como lida ao ser retornada e não volta mais na consulta de não lidas. Se o processamento falhar, ela continua disponível localmente.

Prática	Por que importa
Esvaziar a fila a cada ciclo	A consulta devolve até 200 notificações por vez. Enquanto houver pendentes, a rota deve ser chamada novamente.
Reconciliar periodicamente	A consulta de todas as notificações, filtrada por período, recupera eventos que possam ter se perdido.
Evitar processamento duplicado	Usar o hash e o status para identificar eventos já tratados.
Respeitar o limite de requisições	Excesso de chamadas retorna 429. Usar intervalo fixo de polling e aguardar antes de repetir. Intervalo recomendado e limites: 5 segundos
Consultar antes de agir	A notificação traz apenas o evento; os dados atualizados estão no detalhamento do protocolo.

Rotas do serviço

Resumo do papel de cada rota no fluxo. Parâmetros, campos e exemplos estão na referência técnica.

Nº	Rota	Para que serve e quando chamar
1	POST `/auth/signin` (Eventos)	Obter o token. No início de cada ciclo ou após um 401.
2	GET `/auth` (Eventos)	Verificar se o token ainda é válido (204 válido, 401 inválido).
3	GET `/requirements-notifications` (Eventos)	Buscar as notificações novas. É a rota central do polling.
4	GET `/requirements-notifications/all` (Eventos)	Consultar o histórico de notificações, com paginação e período. Usada na reconciliação.
5	GET `.../requirements/{hash}` (Protocolo)	Ver os dados completos do protocolo, incluindo anexos e indicador de arquivo estruturado.
6	GET `.../requirements` (Protocolo)	Listar e filtrar os protocolos do cartório. Útil para painéis e conferências.
7	GET `.../requirements/file/{id}` (Protocolo)	Baixar um anexo informado no detalhamento.

Nº	Rota	Para que serve e quando chamar
8	GET `.../requirements/{hash}/structured-file` (Protocolo)	Obter os dados do registro em JSON (óbito e nascimento). Só quando houver arquivo estruturado.
9	POST `.../requirements/{hash}/fulfillment` (Protocolo)	Registrar o cumprimento do protocolo.
10	GET `.../requirement/{hash}/historic` (Protocolo)	Ver o histórico de atividades do protocolo.

Nas rotas do serviço Protocolo, `...` corresponde a `/api/v1.0/notifications-system`.

O que o cumprimento exige

O cumprimento é a única rota que altera o protocolo. O corpo é enviado em `multipart/form-data`:

Campo	Obrigatório	Conteúdo
`certificate`	Sim	Tipo da certidão (eletrônica ou física) e, quando eletrônica, a URL da certidão.
`responsibleUser`	Sim	CPF, CNS, nome e e-mail do cartorário responsável.
`subjects`	Não	Lista dos titulares relacionados ao cumprimento.
`file`	Não	Recibo (.pdf, .png, .jpg, .jpeg). Se omitido, o sistema anexa o recibo padrão.

Só é possível cumprir protocolos sob responsabilidade do cartório autenticado e cujo status e pagamento permitam o cumprimento.

Responsabilidades

Parte	Responsabilidades
Oficial do cartório	Gerar e proteger as credenciais; garantir o vínculo do cartório aos tipos de serviço; autorizar os cartorários no IdRC.
Sistema integrador	Executar o polling, persistir e processar as notificações, reconciliar, tratar erros e registrar o cumprimento com dados corretos.

Parte	Responsabilidades
Plataforma e-Protocolo	Disponibilizar os serviços e ambientes, gerar as notificações e manter a referência técnica atualizada.

Segurança e proteção de dados

As respostas do serviço contêm dados pessoais, como nome, CPF, endereço e, no arquivo estruturado de óbito, causa da morte e dados de familiares. Por isso, o tratamento desses dados deve seguir a LGPD:

- Armazenar credenciais, tokens e dados recebidos com controle de acesso.
- Não registrar tokens, senhas ou dados pessoais completos em logs.
- Guardar os dados apenas pelo tempo necessário ao atendimento e às obrigações legais do cartório.
- Trafegar sempre por HTTPS e não compartilhar credenciais entre sistemas ou pessoas.

Índice de regras

ID	Descrição
RN01-Autenticação	O token de acesso vale para as rotas dos serviços Eventos e Protocolo e é enviado no cabeçalho `Authorization: Bearer`.
RN01-Notificações	Cada notificação permanece disponível até ser lida. Ao ser retornada na consulta de não lidas, é marcada como lida e não aparece em consultas seguintes.
RN02-Notificações	Notificações já lidas são consultadas na rota de todas as notificações.
RN01-Arquivo estruturado	O arquivo só é retornado quando o protocolo possui arquivo estruturado vinculado; caso contrário, a rota retorna 404.
RN01-Cumprimento	Somente protocolos sob responsabilidade do cartório autenticado podem ser cumpridos.
RN02-Cumprimento	O cumprimento exige, além do Bearer token, o token do IdRC no cabeçalho `access-token`.
RN03-Cumprimento	O cumprimento só é realizado se o status do requerimento e do pagamento permitirem.

ID	Descrição
RN04-Cumprimento	Se nenhum recibo for enviado, o sistema anexa o recibo padrão.

Glossário

Termo	Definição
Serviço de pendências	Serviço de integração que notifica os cartórios sobre ações do e-Protocolo que exigem intervenção.
Protocolo / requerimento	Solicitação registrada no e-Protocolo, identificada por número e hash.
Hash	Identificador único do protocolo usado nas rotas do serviço Protocolo.
Notificação	Aviso de que ocorreu um evento em um protocolo do cartório.
Polling	Consulta periódica feita pelo sistema do cartório para buscar notificações novas.
Reconciliação	Conferência periódica do histórico de notificações para recuperar eventos não processados.
CNS	Código Nacional de Serventia; identifica o cartório.
Bearer token	Token de acesso obtido na autenticação e enviado no cabeçalho Authorization.
IdRC	Sistema de Autenticação Eletrônica do Registro Civil.
Nota de exigência	Pendência enviada ao solicitante para complementação do protocolo.
Arquivo estruturado	Arquivo JSON com os dados do registro, vinculado ao protocolo.