# Flujo de Integración

La integración con la plataforma del Ministerio de Hacienda para Comprobantes Electrónicos se puede dividir en dos pasos principales:

* Acceder el IDP y obtener un token
* Enviar o consultar un documento electrónico

## IDP

En el caso del IDP (*Identity Provider*) se debe tener claro que se encuentra basado en el estándar OpenID Connect (OIDC); es decir, constituye una extensión de *OAuth 2.0*

Gráficamente, el único código HTTP que permite continuar con el siguiente paso es el HTTP 200.



La línea negra representa los comprobantes q están ok y la línea Rojo representa la basura que se envía a la plataforma

Las respuestas que se pueden brindar son:

|  |  |  |
| --- | --- | --- |
| **Código de HTTP** | **Mensaje de Estado** | **Descripción** |
| **200** | OK | Quiere decir que el IDP retorna el tokenQuiere decir que la petición fue recibida correctamente y se retorna un JSON con la información del *access\_token* y *refresh\_token*, entre otros. |
| **400** | Bad Request | La petición es inválida o mal formada |
| **401** | Unauthorized | El client\_id o token es inválido |
| **403** | Forbidden | Acceso no permitido, El acceso al API está bloqueado |
| **499** | Client Closed Request | La petición no pudo ser recibida por la plataforma. Debe reintentarse el proceso. |
| **50X** | Error | Un error sobre el IDP; en este caso la petición no pudo ser atendida.Corresponde a un error del API, en el X-Error-Cause se debe validar el mensaje. |

## API Recepción

El API de recepción es el que permite enviar o consultar un documento electrónico a la plataforma de Comprobantes. Este posee dos métodos:

En resumen, al enviar un documento a la plataforma se debe esperar un código HTTP 202. Este código es el único que garantiza que el documento ha sido recibido para procesamiento.



De particular importancia el validar el **X-Error-Cause** en las respuestas 400 o 50X; pues ellas indican el motivo por el cual el request es inválido y especialmente cuando se trata del envío de dos o más peticiones de la misma clave en el POST.

**/recepcion, método POST**

|  |  |  |
| --- | --- | --- |
| **Código de HTTP** | **Mensaje de Estado** | **Descripción** |
| **201** | OK | Se recibió correctamente el comprobante electrónico o respuesta del receptor, queda pendiente la validación del mismo y el envío de la respuesta de parte de Hacienda. |
| **400** | Se da algún error de validación | Un ejemplo de esto es cuando envían una clave que ya ha sido recibida. Existe un header que se llama “X-Error-Cause” que retorna la razón. A manera de ejemplo: El comprobante con la Clave [50601011600310112345600100010100000000011999999999] ya fue recibido. |
| **401** | Unauthorized | Si la autorización del token de OAuth es inválida, entonces se recibe un 401. Puede ser porque el client\_id o el token es inválido.  |
| **403** | Forbidden | El acceso al API esta bloqueado |
| **429** | Too Many Requests | El control de límite de cuota ha detenido el envio de un POST. De particular importancia en STAG; el cual tiene límites de 100 POST/GET por hora y de 1000 POST/Get por día |
| **499** | Client Closed Request | La petición no pudo ser recibida por la plataforma. Debe reintentarse el proceso. |
| **50X** | Error | Corresponde a un error del API, en el X-Error-Cause se debe validar el mensaje.  |

Descrito lo anterior, si el contribuyente desea conocer el estado de un documento enviado previamente a la plataforma debe emplear este API.



El código esperado es un 200; pero se debe prestar atención a un HTTP 404; pues este quiere decir que la clave consultada NO existe en la plataforma de Comprobantes. Tal situación se da si el hacer el POST no se recibió un 202; por lo cual carece de sentido hacer invocaciones posteriores al método GET; ya que siempre retornaría un 404.

**/recepcion, método GET**

|  |  |  |
| --- | --- | --- |
| **Código de HTTP** | **Mensaje de Estado** | **Descripción** |
| **200** | OK | Se retorna la información del documento indicado |
| **404** | Not Found | La clave a consultar NO esta en la plataforma de Hacienda; por consiguiente no tiene razón de ser que constantemente se haga un GET cuando se recibe ese código. |
| **401** | Unauthorized | Si la autorización del token de OAuth es inválida, entonces se recibe un 401. Puede ser porque el client\_id o el token es inválido.  |
| **403** | Forbidden | El acceso al API esta bloqueado |
| **429** | Too Many Requests | El control de límite de cuota ha detenido el envio de un POST. De particular importancia en STAG; el cual tiene límites de 100 POST/GET por hora y de 1000 POST/Get por día |
| **499** | Client Closed Request | La petición no pudo ser recibida por la plataforma. Debe reintentarse el proceso. |
| **50X** | Error | Corresponde a un error del API, en el X-Error-Cause se debe validar el mensaje.  |

# Diagrama Completo de Flujo Normal

El siguiente diagrama ilustra el proceso normal para enviar un documento a la plataforma. Sus pasos son:

1. Obtener un token en el IDP, el cual responde con un código HTTP 200
2. Se hace un POST al recurso recepción con los datos del comprobante electrónico a ser enviado; esto responde con un HTTP 202
3. Si se envió un callbackUrl[[1]](#footnote-1)[1] en el post; la plataforma envía la respuesta de aceptación o rechazo a ese URL.
4. Si no se uso el callback; se hace una consulta a la clave por medio de un GET a /recepción/{clave} y se obtiene un HTTP 200.



1. [1] Que debe ser una dirección accesible públicamente por Internet [↑](#footnote-ref-1)