# Manual de integración para consumo de APIs de Firma.gub.uy

### **Autor**

Área de seguridad de la información de Agesic

Fecha de creación

31/01/2023

Tipo de publicación

Guía técnica

## Resumen

El presente documento detalla la integración de "firma.gub.uy" con los sistemas externos. Los sistemas externos que se integren podrán enviar uno o mas documentos PDFs para firmar mediante el consumo de API tipo rest, después se hará una redirección a la url de la plataforma de "firma.gub.uy", para firmar ahí los documentos y retornar nuevamente al sistema externo, recibiendo los documentos firmados.

# Propósito y audiencia

#### Propósito

El presente documento tiene por propósito dar a conocer la descripción técnica del mecanismo de integración entre la plataforma de "firma.gub.uy" con sistemas externos.

#### **Audiencia**

Dirigido a técnicos, funcionales y desarrolladores.

## Integración

La plataforma firma.gub.uy permite firmar documentos PDF usando dispositivos locales (cédula de identidad electrónica o etokens) y servicios en la nube (actualmente TuID de Antel e Identidad Mobile de Abitab). La integración es independiente del medio de firma elegido por el usuario. A efectos de ilustrar el procedimiento de integración de un sistema externo con la plataforma se mostrará las interacciones utilizando el aplicativo de firma y la firma en la nube. Por sistema externo se en en en en a qui en aplicación web, funcionando bajo cualquier plataforma, sistema operativo y arquitectura, y desarrollada en cualquier lenguaje de programación, que sea capaz de consumir servicios web de tipo rest y que pueda exponer un recurso web (una página, servlet u otro mecanismo) al cual la plataforma de firma electrónica pueda hacerle un GET a los efectos de notificarle (retornar) cuando el proceso de firma esté finalizado.

Estrictamente hablando, también pueden ser sistemas externos que se integren con "firma.gub.uy" cualquier otra aplicación, aunque no sea web, siempre que pueda consumir servicios web(rest). En este caso, como la aplicación no podrá exponer un recurso web donde la plataforma de firma electrónica pueda notificarle, será responsabilidad de la aplicación hacer un polling constan-te preguntando por el estado del proceso de firma, hasta obtener como respuesta el documento firmado. Esto no es aconsejable por la sobrecarga que produce sobre la red y sobre el servidor dela firma.gub.uy.

#### Descripción general

En la siguiente imagen se muestra la iteración completa entre los sistemas externos, plataforma firma.gub.uy, APIs para los sistemas externos, y aplicativo de firma o firma en la nube, estos 2 últimos según corresponda. describiendo de forma visual el flujo a seguir en cada etapa del proceso de firma, desde su inicio hasta su fin.

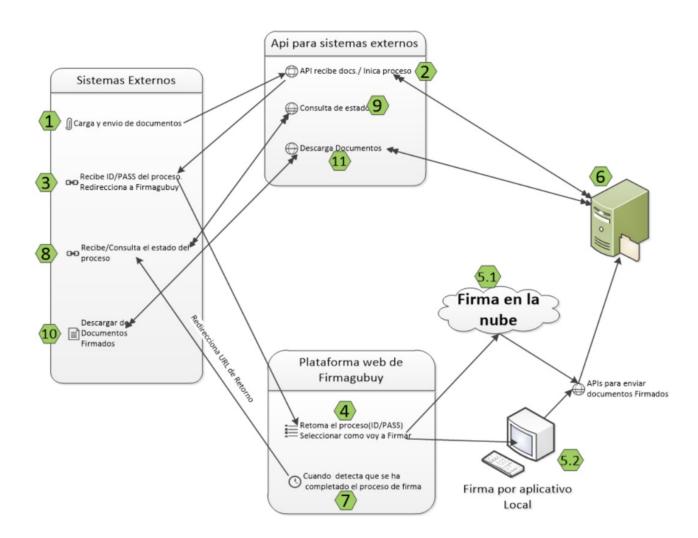


Figura 1. Flujo de firma.gub.uy con sistemas externos

## Descripción del proceso

Carga y envio de documentos. El sistema externo carga y envía uno o mas documentos PDF para firmar. El envío de documentos se puede hacer de dos formas:

a. Envío de documentos en base64 dentro de un json e invocando la api de tipo POST"/api/v1/externos/proceso1", un ejemplo es:

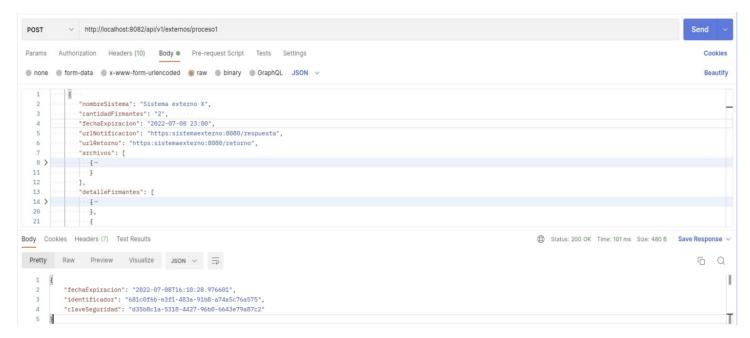


Figura 2. Ejemplo de iniciar proceso base64

b. Envio de documentos utilizado 2 apis, la primera "carga de archivo" api "/api/v1/ex-ternos/archivo" envía cada documento y devuelve un identificador de documento que después se utilizará para iniciar el proceso de firma, los identificadores de archivos van dentro de un json y se envían a la api "/api/v1/externos/proceso2", los ejemplos de lo anterior son:

Carga de archivo.

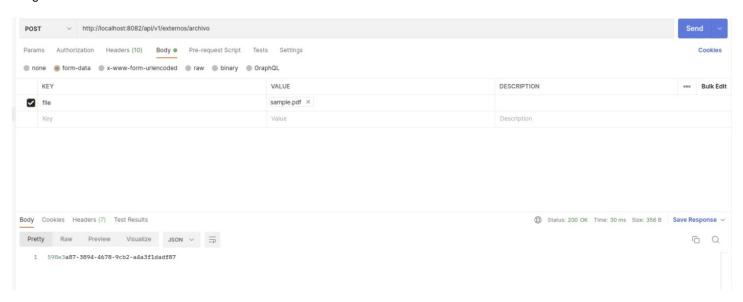


Figura 3. Ejemplo de carga de archivo (uno por uno)

Envío de Json con los iden Oficadores de archivos, previamente cargados

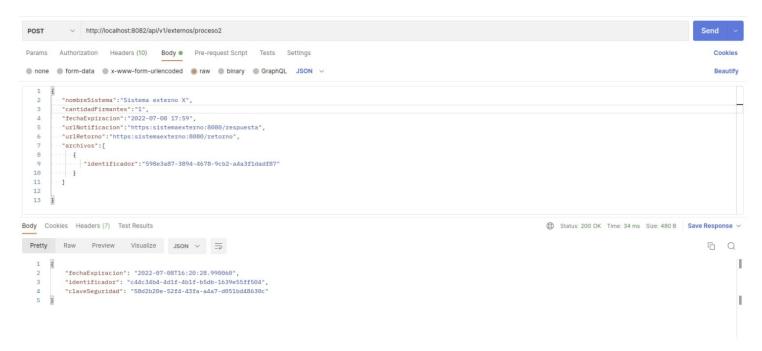


Figura 4. Ejemplo de iniciar proceso con los identificadores de archivos.png

En el body en ambos procesos se debe de agregar algunas propiedades opcionales, nombreSistema, cantidadFirmantes, fechaExpiracion, urlNotificacion, urlNetorno. Se amplía esto más adelante en la documentación de cada api.

Las apis de inicio de proceso devuelvén un identificador, claveSeguridad y fechaExpiracion, siendo el identificador y claveSeguridad necesarios para identificar al proceso defirma.

#### Redirección a "firma.gub.uy"

Una vez que la aplicación externa comenzó un proceso de firma, obtiene como resultadoun identificador y una clave de seguridad, el usuario del sistema externo debe ser redirigido a una página específica de la plataforma para que pueda realizar la firma del documento.

Esta página es identificada por la siguiente URL:

https://<host>:<port>/es/pp/firmar?id=c44c34b4-4d1f-4b1f-b5db-1639e55ff504&pass=58d2b20e-52f4-43fa-a4a7-d051bd48630c

Donde "c44c34b4-4d1f-4b1f-b5db-1639e55ff504" debe ser sustituido por el identificador del proceso y "58d2b20e-52f4-43fa-a4a7-d051bd48630c" es la clave de seguridad, asignado por la plataforma al proceso de firma.

#### En la plataforma de "firma.gub.uy".

- La plataforma identifica el proceso de firma por medio de "id" y "pass" pasados comoparametros.
- Dentro de la plataforma el usuario debe de elegir como quiere firmar, la plataformaguiará dependiendo su elección
- En el caso que seleccione firmar con Antel o Abitab la firma se completara en la plataforma de ellos, siguiendo los pasos que se indiquen, como punto final este proceso incluye el envío de los documentos firmados al servidor.
- Si selecciona firmar con dispositivo, tendrá las opciones de firmar con cédula, tokenabitab o token correo, en todos estos
  casos la firma se hará descargando un archivocon extensión ".firmagubuy" que la plataforma le guiara hasta llegar a la
  descarga. Luego se abrirá este archivo el cual a su vez abre al aplicativo de firma en donde se completará la firma. Como
  punto final el aplicativo de firma enviara al servidor los archivos firmados mediante apis.

#### La plataforma detecta que se ha completado el proceso de firma

La plataforma de "firma.gub.uy", se quedó esperando, cuando detecta que el proceso defirma ha sido completado, la plataforma hará una redirección hacía la url de retorno pro-porcionada al inicio del proceso de firma, agregando como parámetro el estado del proce-so de firma.

#### De regreso al sistema externo

El sistema externo, podra consultar el estado del proceso de firma (si lo es\textit{Oma convenien-te}) haciendo esto por medio del api

"{URL}/api/v1/externos/estado/681c0f6b-e3f1-483a-91b8-a74a5c76a575", se detalla un ejemplo en la siguiente imagen.

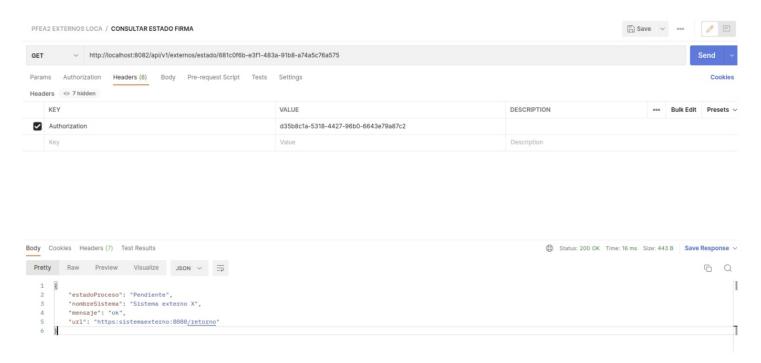


Figura 5. Ejemplo de consulta de estado de proceso de firma

#### Descarga de documentos

El sistema externo invoca el api para descargar los documentos, aquí tiene 2 opciones.

Descargar documento uno a uno, invocando la api"{URL}/api/v1/externos/archivo/598e3a87-3894-4678-9cb2-a4a3f1dadf87", siendo en este caso '598e3a87-3894-4678-9cb2-a4a3f1dadf87" el identificador de archivo que deseamos descargar. Para usar esta op-ción se debe de iniciar el proceso de firma desde el api "/api/v1/externos/proceso2" y el sistema externo debe de guardar los iden\text{\text{Gicadores}} de archivos asociados al pro-ceso, para pedir los archivos individualmente por medio de estos. (ver documentaciónde api)



Figura 6. Ejemplo de descarga de archivo (individual)

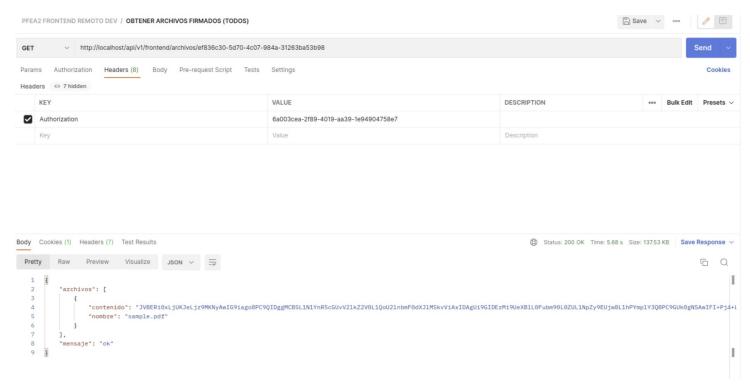


Figura 7. Ejemplo de obtener documentos firmados (todos).png

# Descripción de APIS

## Iniciar proceso de firma

Datos generales								
Descripción	Permite a los otros datos.	Permite a los sistemas externos generar un proceso de firma a partir de uno o más archivos y otros datos.						
Método HT	POST	POST						
Path	/api/externos	/proceso1						
Entrada	application/js	on						
Salida	application/js	on						
Parámetros de entrad	a							
		Obligatorio; debe con	tener al	menos un archivo.				
archivos	Lista de archivos	nombre	Texto	Obligatorio; nombre del archivo.				
		contenido	Bytes	Obligatorio; contenido del archivo, en formato Base64.				
nombre_sistema	Texto	Obligatorio; nombre o para auditoría.	lel sisten	na que inicia el proceso, para mostrar al usuario y				
firma_longev	Si/No	onal; indicador de si s asume que no se utili		re utilizar firma longeva o no. Si no se es especifica s longeva.				
cantidad_firmante	Entero	pcional; cantidad de firmas que deben efectuarse sobre el archivo. Si no se proporciona, se asume "1". Si se proporciona elvalor "0", no se limita la cantidade firmantes.						
		cada uno de los usua los firmantes en exce	rios. Si e -so será: es. Si el l tes en ex					
		documento_numero	Texto	Opcional; número de documento de la persona que debe firmar. Sise proporciona, el API debe validar que la persona que firma el archivo pueda ser identificada con el mismo número en el certificado digital que usa para firmar.				
detalles_firmante	Lista defirmantes	documento_pais	Texto	Opcional; código ISO2 del país emisor del documento de la persona que debe firmar. Si se proporciona el parámetro documento_numero pero no se proporciona este parámetro, se asume "UY"(Uruguay).				

		documento_tipo	Texto	Opcional; tipo de documento, según el catálogo de tipos de documentos que determine AGESIC. Sise proporciona el parámetro documento_numero pero no se proporciona este parámetro, se asume el valor que corresponda a la cédula de identidad.			
			forzar_cedula	Sí/No	Opcional; indicador de si se debe forzar que la firma de los archivos sea realizada utilizando una cédula de identidad electrónica o no. Si se omite, se asume "No".		
			validar_firmante	Sí/No	Opcional; indicador de si se debe validar que la persona que firma puede identificarse mediante el certificado digital. Si se omite, se asume "No".		
fecha	ı_limite	Fecha yhora	Opcional; fecha y hora límites para que el proceso de firma seacompletado. Si se proporciona, el API puede limitarlo a un período menor, según configuración. Si no se proporciona, el API debe asignarle un valor, según configuración.				
url_n	url_notificación URL		Opcional; URL a donde la plataforma de firma debe notificar queel proceso de firma fue completado. El recurso detrás de esta URL debe aceptar el método POST, incluyendo en el cuerpo (body) del mensaje los siguientes parámetros en formato JSON:identificador: idenθficador del proceso de firma finalizado (UUID).estado: estado del proceso de firma ('FINALIZADO', 'RECHAZADO'). Si se omite, el sistema externo no podrá ser noθficado cuando elproceso de firma se complete, debiendo hacer polling constante utilizando el método de consulta de estado.				
url_re	etorno	URL	Opcional; URL a la cual la plataforma de firma debe redirigir alusuario luego de que éste complete la firma de los archivos. (seespera que el sistema externo pueda continuar con su proceso,ya sea incluyendo un identificador en la propia URL o tomandolos datos de la sesión, o de otra manera, a su criterio). Si no seespecifica, al finalizar el proceso de firma el usuario quedaráviendo una pantalla de confirmación propia de la plataforma.				
Pará	metros de salida						
	identificador	UUID	Identifica unívocame	nte a un ¡	proceso de firma.		
	Clave_seguridad	Texto	Clave de seguridad que deberá ser proporcionada para consultarel estado del proceso de firma y obtener los archivos firmados.				
200	fecha_expiracion	Fecha y hora	plataforma, de la sigui "fecha_limite", se cal configuración denom parámetro "fecha_limitecha es menor oigui "PLAZO_MAXIMO_E incluye el parámetro ahora y dicha fecha e	uiente ma cu-la con iinado "Pl nite", y el al a un pa EXPIRAC "fecha_lii es ma-yo EXPIRAC netro de c			
400 Mensaje Texto		Mensaje explicativo en el caso de fallo.					

## Iniciar proceso de firma (solo metadatos)

#### **Datos generales**

Descripción	tener en cuenta	Permite a un sistema externo cargar un único archivo, obteniendo un identificador para el mismo. Se debe tener en cuenta que aún no se generó un proceso de firma para este archivo, sino que se hará posteriormente cuando se hayan cargado todos los archivos correspondientes.					
Método HTTP	POST	POST					
Path	/api/externos/arc	hivo					
Entrada	application/octet	-stream					
Salida	application/json						
Parámetros	de entrada						
archivo	Archivo	Obligatorio; e	el archivo debe ser pasado en formato binario.				
nombre	Texto Obligatorio; debe ser pasado usando el header "Content-Disposition".						
Parámetros	Parámetros de salida						
200	identificado	UUID	Identifica unívocamente a un archivo.				
400	mensaje	Texto	Mensaje explicativo en el caso de fallo.				

## Iniciar proceso de firma

Datos generales						
Descripción		Permite a los sistemas externos generar un proceso de firma a partir de uno o más archivos cargados previamente utilizando el endpoint "Cargar archivo".				
Método HTTP	POST					
Path	/api/exter	rnos/proceso2				
Entrada	application	on/json				
Salida	application	on/json				
Parámetros de enti	rada					
archivos	Lista de identifi-cadores	Obligatorio; debe contener al menos un identificador, y todos ellos deben corresponderse a archivos cargados previamente utilizando el endpoint "Cargar archivo" y que no estén asociados aún a ningún proceso de firma.				
nombre_sistema	Texto	Obligatorio; nombre del sistema que inicia el proceso, para mos- trar al usuario y para auditoría.				
firma_longeva	Sí/No	Opcional; indicador de si se requiere utilizar firma longeva o no. Si no se es especifica se asume que no se utiliza firma longeva.				
	Entero	Opcional; cantidad de firmas que deben efectuarse sobre el ar- chivo. Si no se proporciona, se asume "1". Si se proporciona el valor "0", no se limita la cantidad de firmantes.				
cantidad_firmantes	Entero	Opcional; cantidad de firmas que deben efectuarse sobre el ar- chivo. Si no se proporciona, se asume "1". Si se proporciona el valor "0", no se limita la cantidad de firmantes.				

Opcional; detalles sobre los firmantes, para mostrar antes de proceder a la firma de cada uno de los usuarios. Si el largo de la lista es menor a la cantidad de firmantes, los firmantes en exce- so serán tratados como anónimos, con los valores asumidos para todas las variables. Si el largo de la lista es mayor a la cantidad de firmantes, se ignoran los firmantes en exceso.

Para cada firmante se debe especificar:

		Lista de firman- tes				
			documento_numero	Texto	Opcional; número de documento de la persona que debe firmar. Si se proporciona, el API debe validar que la persona que firma el archi- vo pueda ser identificada con el mismo número en el certificado digital que usa para firmar.	
detal	lles_firmantes		documento_pais	Texto	Opcional; código ISO2 del país emisor del documento de la per- sona que debe firmar. Si se pro- porciona el parámetro documen- to_numero pero no se proporcio- na este parámetro, se asume "UY" (Uruguay).	
			documento_tipo	Texto	Opcional; tipo de documento, se- gún el catálogo de tipos de docu- mentos que determine AGESIC. Si se proporciona el parámetro docu- mento_numero pero no se pro- porciona este parámetro, se asu- me el valor que corresponda a la cédula de identidad.	
			forzar_cedula	Sí/No	Opcional; indicador de si se debe forzar que la firma de los archivos sea realizada utilizando una cédula de identidad electrónica o no. Si se omite, se asume "No".	
			validar_firmante	Sí/No	Opcional; indicador de si se debe validar que la persona que firma puede identificarse mediante el certificado digital. Si se omite, se asume "No".	
fecha	a_limite	Fecha y hora	Opcional; fecha y hora límites para que el proceso de firma sea completado. Si se proporciona, el API puede limitarlo a un perío- do menor, según configuración. Si no se proporciona, el API debe asignarle un valor, según configuración.			
		URL	Opcional; URL a donde la plataforma de firma debe notificar que el proceso de firma fue completado. El recurso detrás de esta			
			URL debe aceptar el método POST, incluyendo en el cuerpo (body) del mensaje los siguientes parámetros en formato JSON:			
uri_n	otificacion				or del proceso de firma finaliza- do (UUID). eso de firma ('FINALIZADO', 'RE- CHAZADO').	
			Si se omite, el sistema externo no podrá ser notificado cuando el proceso de firma se complete, debiendo hacer polling constante utilizando el método de consulta de estado.			
url_retorno		URL	complete la firma de proceso, ya sea inclu sesión, o de otra mar	los archiv Iyendo ur nera, a si	taforma de firma debe redirigir al usuario luego de que éste vos. (se espera que el sistema externo pueda continuar con su nidentificador en la propia URL o tomando los datos de la u criterio). Si no se especifica, al finalizar el proceso de firma el pantalla de confirmación propia de la plataforma.	
Pará	metros de sali	da				
	identificador	UUID	Identifica unívocame	nte a un	proceso de firma.	
	clave_segu- ridad	Texto	Clave de seguridad o firma y obtener los ar		rá ser proporcionada para consultar el estado del proceso de rmados.	

Fecha y hora de expiración del proceso de firma. Esta fecha es

calculada por la plataforma, de la siguiente manera:

Si la invocación no incluye el parámetro "fecha\_limite", se calcula como (ahora + N minutos), donde N es un pa- rámetro de configuración denominado "PLAZO\_EXPIRA-CION".

200

fecha_expi-	Fecha y
racion	hora

- Si la invocación incluye el parámetro "fecha\_limite", y el mismo es válido (la diferencia entre ahora y dicha fecha es menor o igual a un parámetro de configuración denominado "PLAZO\_MAXIMO\_EXPIRACION"), entonces es la misma fecha.
- Si la invocación incluye el parámetro "fecha\_limite", pero el no mismo es válido (la
  diferencia entre ahora y dicha fecha es mayor a un parámetro de configuración
  denominado "PLAZO\_MAXIMO\_EXPIRACION"), entonces se calcula como (ahora + N
  minutos), donde N es un pa- rámetro de configuración denominado "PLAZO\_MAXIMO\_EXPIRACION".

400	mensaje	Texto	Mensaje explicativo en el caso de fallo.
-----	---------	-------	--

#### Consultar estado del proceso de firma.

Datos gen	erales		
Descripción	า		e al módulo frontend o sistemas externos consultar el es- tado de un proceso de firma (pendiente, etado, obsoleto).
Método HT	TP	HEAD	
Path		/api/ext	ternos/estado/{identificador}
Entrada		No tien	ne
Salida		applica	ation/json
Parámetro	s de er	ntrada	
identificado	or	UUID	Obligatorio; identificador del proceso de firma que se desea consultar.
clave_segu	ıridad	Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma; debe ser pasado utilizando el en- cabezado "Authorization".
Parámetro	s de sa	alida	
200		json	Devuelve un json con la siguiente información: es- tadoProceso, nombreSistema, mensaje y url de re- torno.
304 mer	nsaje	Texto	Sin Mensaje
403 mer	ısaje	Texto	Mensaje indicando que la clave de seguridad no es correcta.
404 men	nsaje	Texto	Mensaje indicando que el proceso de firma no existe o ya está expirado.

Dates	generales				
Descri	pción	Permite al m	nódulo frontend obtener todos los archivos firmados corres- pondientes a un proceso de firma.		
Método	o HTTP	GET			
Path		/api/externo:	os/archivos/{identificador}		
Entrad	a	No tiene			
Salida		application/j	json		
Parám	etros de e	ntrada			
identifi	cador	UUID	Obligatorio; identificador del proceso de firma para el cual se desean obtener los archivos firmados.		
clave_	seguridad	Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma; debe ser pasado utilizando el encabezado "Authoriza- tion".		
Parám	etros de s	alida			
			Lista de archivos firmados. Para cada archivo se proporicionan los siguientes datos:		
200	archivo	Lista de archivos	nombre Texto Nombre original del archivo.		
			contenido Bytes Contenido del archivo, en formato Ba- se64.		
304	mensaje	Texto	Sin mensaje.		
403	mensaje	Texto	Mensaje indicando que la clave de seguridad no es correcta.		
404	mensaje	Texto	Mensaje indicando que el proceso de firma no existe o ya está expirado.		

## Obtener archivo firmado(forma individual)

Datos generales								
Descripción	Permite	Permite al modulo frontend obtener unos archivos firmados correspondietes a un proceso de firma						
Método HTTP	GET							
Path	/api/exte	rnos/archivos/{identificador}						
Entrada	No tiene							
Salida	application/octet-stream							
Parámetros de e	ntrada							
identificador	UUID	Obligatorio; identificador del archivo para el cual se desea obtener su correspondiente archivo firmado.						
clave_seguridad	Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma al cual pertenece el archivo; debe ser pasado utilizando el encabezado "Authoriza- tion".						
Parámetros de salida								
200 archivo	Archivo	Archivo firmado. El contenido del archivo se de- vuelve en formato binario, mientras que el nombre del mismo se informa a través del header "Content-Disposition".						

304	mensaje	Texto	Sin Mensaje
403	mensaje	Texto	Mensaje indicando que la clave de seguridad no es correcta.
404	mensaje	Texto	Mensaje indicando que el proceso de firma no existe o ya está expirado.

#### Obtener Información sobre las firmas de un archivo.

Datos	s generales		
Desci	ripción	Permite	al módulo frontend obtener un archivos firmados co- rrespondiente a un proceso de firma.
Méto	do HTTP	GET	
Path		/api/exte	rnos/archivo/{identificador}
Entra	da	No tiene	
Salida	a	application	on/octet-stream
Parár	netros de e	ntrada	
identi	ficador	UUID	Obligatorio; identificador del archivo para el cual se desea obtener su correspondiente archivo fir- mado.
clave	_seguridad	Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma al cual pertenece el archivo; debe ser pasado utilizando el encabezado "Authoriza- tion".
Parár	netros de s	alida	
200	archivo	Archivo	Archivo firmado. El contenido del archivo se devuelve en formato binario, mientras que el nombre del mismo se informa a través del header "Con- tent-Disposition".
304	mensaje	Texto	Sin mensaje
403	mensaje	Texto	Mensaje indicando que la clave de seguridad no es correcta.
404	mensaje	Texto	Mensaje indicando que el proceso de firma no existe o ya está expirado.

## **Anexos**

1. Se agrega anexo de colecciones de postman para cada una de las api de sistemas externos