



PROTOCOLO DE CONEXIÓN A REPOSITORIO DE FIRMAS
DOCUMENTACIÓN TÉCNICA INTEGRACIÓN API
REPOSITORIO CENTRALIZADO DE FIRMAS
VERSIÓN 8

29/01/2020

Índice

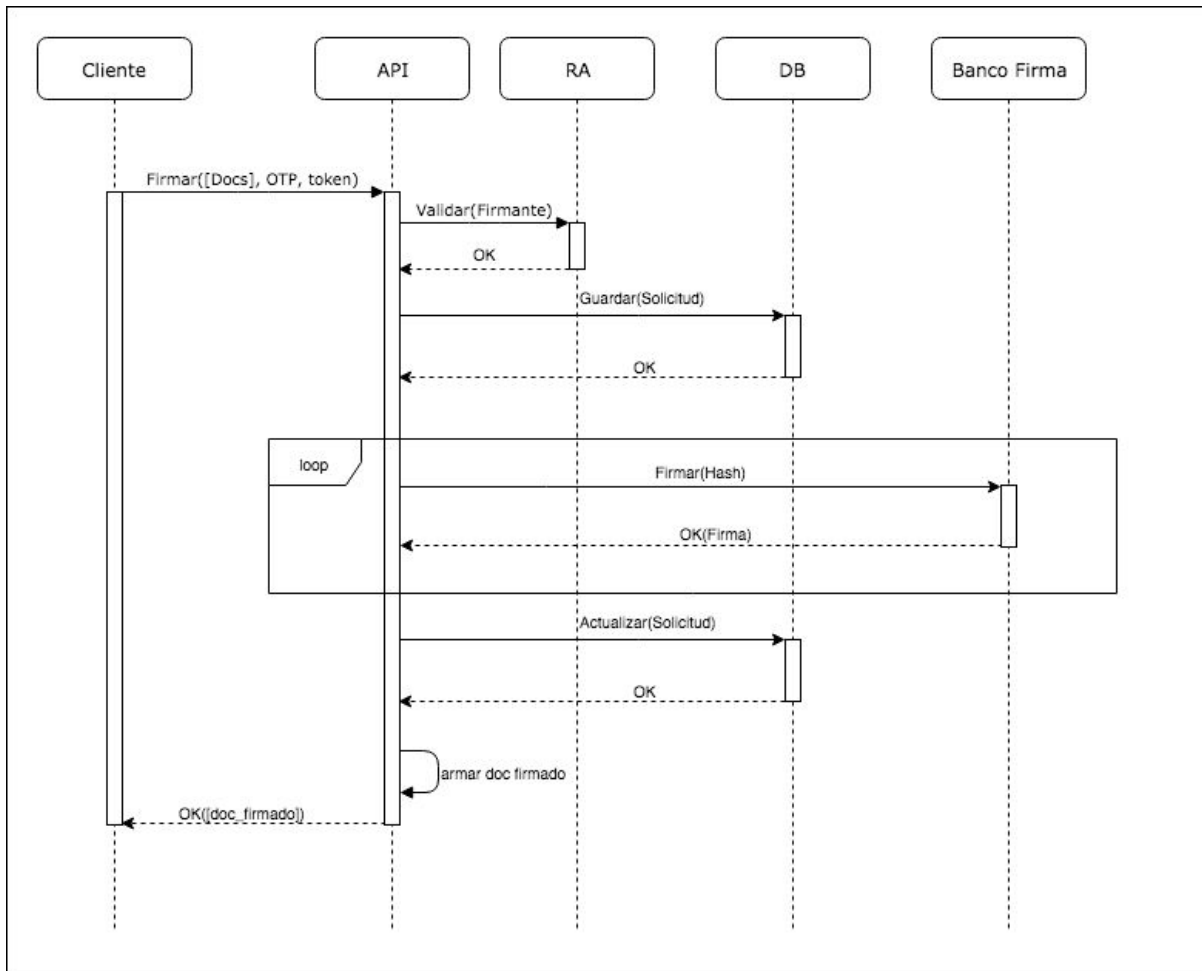
Introducción	3
Diagrama de secuencia	4
Firmar Documento	6
Ambiente de TEST	13
Firma atendida	13
Firma desatendida	14
Códigos HTTP asociados a la API	15
Instalación aplicación móvil y configuración OTP	17
Aplicación OTP	17
Configuración para incrustar firma a PDF	18
Definiciones y acrónimos	21
Historial de cambios	22
Clasificación del documento	22

1. Introducción

Este documento contiene la documentación de los mecanismos para que aplicaciones desarrolladas por las instituciones puedan realizar procesos de firma de documentos utilizando las firmas electrónicas avanzadas de autoridades o funcionarios custodiadas en el Repositorio Centralizado de Firmas.

2. Diagrama de secuencia

A continuación se presenta el diagrama correspondiente a las acciones a realizar con el objetivo de obtener uno o más documentos firmados.



- **Cliente:** Aplicación cliente que requiere firmar uno o más documentos.
- **API Firma:** Interfaz entre las aplicaciones externas (clientes) y las operaciones asociadas a la firma de uno o más documentos.
- **RA (Autoridad de Registro):** Contiene el registro de las aplicaciones externas habilitadas para realizar operaciones de firma. Las aplicaciones deben estar previamente registradas y cumplir con un conjunto de restricciones asociadas a la identificación del certificado de firma electrónica avanzada a utilizar (**entidad, propósito y run** del titular de la firma).

- **Banco:** Repositorio donde se custodian los certificados de firma electrónica avanzada habilitados para realizar operaciones de firma. El banco recibe los documentos a firmar y realiza la operación de firma, **nunca un certificado será expuesto.**

Firmar Documento

Con esta llamada, se puede firmar documentos PDF, XML o hash, utilizando un certificado de firma electrónica avanzada de propósito general (atendida) o desatendido.

Para utilizar su firma desatendida, previamente tendrá que haber solicitado su certificado por el "Sistema de Solicitud de Firma Electrónica" y habilitado la aplicación correspondiente.

En el caso de firmar un PDF, el proceso tomará más tiempo ya que se requiere manipular el documento para incrustar la firma. La recomendación es firmar un hash, pero es necesario que la aplicación cliente reconstruya el documento. Si necesita ayuda con la firma de hash póngase en contacto con soporte.

Protocolo: HTTPS

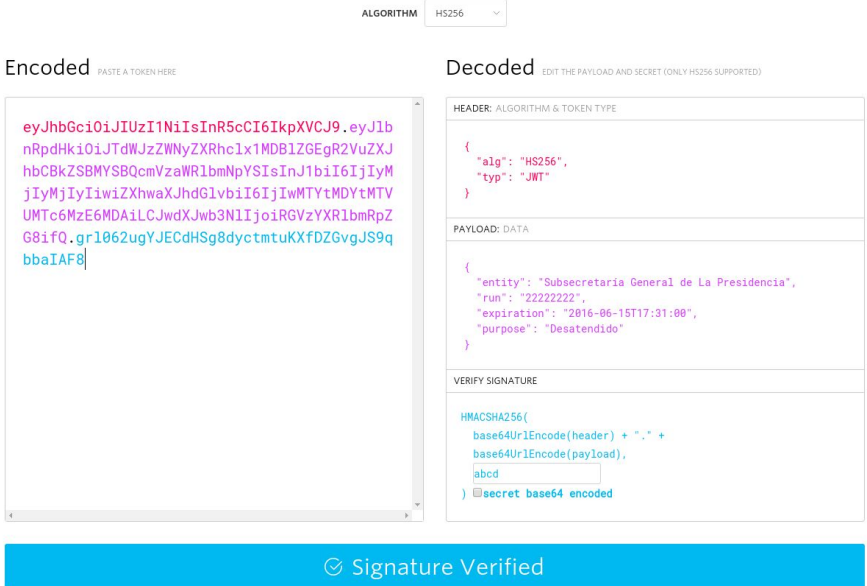
URL: [https://api-firma-v2.test.digital.gob.cl/firma/v2/files/tickets'](https://api-firma-v2.test.digital.gob.cl/firma/v2/files/tickets),
método = ['**POST**']

HTTP Headers

OTP: <Valor OTP> (Esta cabecera sólo es necesaria para la firma atendida, en caso de ser firma desatendida, no se debe enviar esta cabecera).

HTTP Parámetros

token	<p>Campo encriptado y firmado en JWT con una clave simétrica, esta clave es obtenida a partir del registro de la aplicación.</p> <p>El campo JWT encriptado en algoritmo HS256 y firmado con clave simétrica contiene los siguientes campos:</p> <ol style="list-style-type: none">1. run: run identificador del titular de firma, no debe contener puntos, guión ni tampoco el dígito verificador (string).2. entity: código asociado a la institución a la cual pertenece el titular (string)3. purpose: código asociado al tipo de certificado a utilizar
--------------	---

	<p>(string)</p> <p>4. expiration: fecha expiración del token en hora chilena formato ISODate (YYYY-MM-DDTHH:MM:SS). No puede ser mayor a 30 minutos del momento actual.</p> 																					
<p>api_token_key</p>	<p>Campo no encriptado de tipo string que contiene el código único generado a partir del registro de la aplicación.</p>																					
<p>files</p>	<p>Array no encriptado que contiene información de el o los documentos sobre los cuales se realizarán operaciones de firma. Cada objeto del array según el formato de archivo a firmar debe contener:</p> <table border="1" data-bbox="474 1360 1409 1827"> <thead> <tr> <th>JSON</th> <th>PDF</th> <th>XML</th> </tr> </thead> <tbody> <tr> <td>description</td> <td>description</td> <td>description</td> </tr> <tr> <td>checksum</td> <td>checksum</td> <td>checksum</td> </tr> <tr> <td>content</td> <td>content</td> <td>content</td> </tr> <tr> <td>content-type</td> <td>content-type</td> <td>content-type</td> </tr> <tr> <td></td> <td>layout (opcional ver Anexo B)</td> <td>references</td> </tr> <tr> <td></td> <td></td> <td>xmlObjects</td> </tr> </tbody> </table> <p>A continuación se describe el tipo de dato asociado al parámetro</p>	JSON	PDF	XML	description	description	description	checksum	checksum	checksum	content	content	content	content-type	content-type	content-type		layout (opcional ver Anexo B)	references			xmlObjects
JSON	PDF	XML																				
description	description	description																				
checksum	checksum	checksum																				
content	content	content																				
content-type	content-type	content-type																				
	layout (opcional ver Anexo B)	references																				
		xmlObjects																				

	<p>requerido:</p> <ol style="list-style-type: none"> 1. description: string con la descripción del archivo 2. checksum: SHA256 del archivo 3. content: archivo en base64 4. content-type: dependiendo del archivo a firmar <ol style="list-style-type: none"> i. application/pdf ii. application/xml iii. application/json 5. layout: string opcional en caso de desear incrustar elemento al archivo PDF 6. references: array de string con la identificación del nodo a firmar en caso de ser un archivo XML ejemplo: ["#nodo1", "#nodo2"] 7. xmlObjects: array de string con los pie de firma en un archivo XML ejemplo: ["<a>",""]
--	---

A continuación se presentan ejemplos de los parámetros:

token	<pre>"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbmRpdHkiOiJTdWJzZWNYZXRhclx1MDBlZGEgR2VuZlJhbCBkZSBMYSBQcmVzaWRlbnNpYSIsInJ1biI6IjlyMjlyMjlyIiwiaXhwaXJhdGlvbil6IjIwMTYtMDYtMTVUMTc6MzE6MDAiLCJwdXJwb3NlIjoieGVzYXRlbnRpdG8ifQ.grl062ugYJECdHSg8dyctmtuKXfDZGvgJS9qbbalAF8"</pre> <p><i>Algoritmo: HS256, Secreto: abcd</i></p> <pre>{ "entity": "Subsecretaría General de La Presidencia", "run": "22222222", "expiration": "2016-06-15T17:31:00", "purpose": "Desatendido" }</pre>
api_token_key	<i>sandbox</i>
files	<pre>[{ "content-type": "application/pdf", "content": "archivo en base64", "description": "str", "checksum": "hash en sha256" }]</pre>

Ejemplo del JSON BODY para firmar un documento PDF:

```
{  
  "api_token_key": "sandbox",  
  "token":  
  "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbnRpdHkiOiJTdWJzZWNYZXRhclx1MDBIZGEGR2VuZXJhbCBkZSBMYSBQcmVzaWRlbnNpYSIsInJ1biI6IjIyMjIyMjIyIiwiaXNjaXhwaXJhdGlvb2I6IjIwMTYtMDYtMTVUMTc6MzE6MDAiLCJwdXJwb3NIIjoiaGVzYXRlbnRpdG8ifQ.grl062ugYJECdHSg8dyctmtuKXfDZGvgJS9qbbaIAF8",  
  "files": [  
    {  
      "content-type": "application/pdf",  
      "content": "archivo en base64",  
      "description": "str",  
      "checksum": "hash en sha256"  
    }  
  ]  
}
```

Response Json Schema Body

El resultado de este llamado corresponde a un JSON que contiene los documentos firmados.

```
{  
  "$schema": "http://json-schema.org/draft-04/schema#",  
  "description": "Recepción de documentos firmados",  
  "type": "object",  
  "required": [  
    "session_token",  
    "files"  
  ],  
  "additionalProperties": false,  
  "properties": {
```

```
"session_token": {  
  "type": "string"  
},  
"metadata": {  
  "type": "object",  
  "properties": {  
    "OTP_expired": {  
      "type": "boolean"  
    },  
    "files_recived": {  
      "type": "number"  
    },  
    "files_signed": {  
      "type": "number"  
    },  
    "signed_failed": {  
      "type": "number"  
    }  
  },  
  "required": [  
    "OTP_expired",  
    "files_received",  
    "files_signed",  
    "signed_failed"  
  ]  
},  
"files": {  
  "type": "array",  
  "minItems": 1,  
  "items": {  
    "type": "object",  
    "required": [  
      "checksum_original",  
      "status"  
    ],  
    "additionalProperties": false,
```

```
"properties": {  
  "type": {  
    "enum": [  
      "PDF",  
      "JSON",  
      "XML"  
    ]  
  },  
  "content": {  
    "type": "string"  
  },  
  "checksum_original": {  
    "type": "string"  
  },  
  "checksum": {  
    "type": "string"  
  },  
  "description": {  
    "type": "string"  
  },  
  "status": {  
    "type": "string"  
  }  
}  
}  
}  
}  
}
```

Un ejemplo de respuesta es la siguiente:

```
{  
  "files": [  
    {  
      "checksum_original":  
"447ac80f0d813be18d2ad59db26c4167198b656d356bd1b47ccd131d617165  
27",
```

```

    "status": "error"
  },
  {
    "checksum_original":
"453ac80f0d813be18d2ad59db26c4167198b656d356bd1b47ccd131d617165
27",
    "Content": "YXNkYXNkc2FkYXNk"
    "status": "OK"
  }
],
"metadata": {
  "signed_failed": 1,
  "OTP_expired": false,
  "files_signed": 0,
  "files_received": 1
}
}

```

En el campo files se recibe una lista de objetos, este contiene lo siguiente:

checksum_original	SHA256 del archivo original.
checksum_signed	SHA256 del archivo firmado, siempre y cuando se logre firmar el archivo
status	error - no se concretó la firma
	OK - transacción correcta
content	base64 del archivo firmado

En el campo metadata se recibe un objeto que contiene lo siguiente:

signed_file	número de archivos firmados
OTP_expired	booleano que indica si el OTP se pudo usar de manera correcta con la totalidad de archivos
files_signed	Número de archivos que se pudieron firmar
files_recived	Número de archivos recibidos

3. Ambiente de TEST

Las firmas generadas en este ambiente no son válidas, es sólo para facilitar la integración.

Firma atendida

api_token_key	sandbox
JWT	<pre>{ "purpose": "Propósito General", "entity": "Subsecretaría General de La Presidencia", "expiration": "2016-06-15T17:31:00", "run": "11111111" }</pre>
secreto	abcd

El código QR correspondiente a semilla para generar OTPs asociadas a este certificado es el siguiente:



En el Anexo A se detalla cómo realizar la instalación y configuración para la generación de OTPs.

Firma desatendida

api_token_key	sandbox
JWT	<pre>{ "purpose": "Desatendido", "entity": "Subsecretaría General de La Presidencia", "expiration": "2016-06-15T17:31:00", "run": "22222222" }</pre>
secreto	abcd

En el caso de firma desatendida no debe enviarse el header OTP.

4. Códigos HTTP asociados a la API

Revisa la siguiente URL para probar la API:
<https://api-firma-v2.test.digital.gob.cl/swagger-ui.html#>

Recurso: `/v2/files/tickets`

Status code	Tipo	Response
200	Ok	<code>{"session_token": string}</code>
400	Bad request	<code>{"error": "Petición mal formada"}</code>
401	Token mal formado, no válido, etc.	<code>{"error": "El token generado fue alterado durante el envío del mensaje"}</code>
409	Archivo corrupto	<code>{"error": "El checksum calculado no corresponde al enviado"}</code>
412	Expirado	<code>{"error": "Ticket expirado"}</code>
500	Error interno	<code>{"error": "Error Interno"}</code>

Status code	Response
200	<code>{"files": [{"checksum_original": "SHA256", "status": "error "OK", "checksum_signed": "SHA256", "content": base 64}], "metadata": {"signed_failed": int, "OTP_expired": boolean, "files_signed": int, "files_received": int}, "session_token": string}</code>
206	<code>{"files": [{"checksum_original": "SHA256", "status": "error "OK", "checksum_signed": "SHA256", "content": base 64}], "metadata": {"signed_failed": int, "OTP_expired": boolean, "files_signed": int,</code>

	<pre>"files_received": int}, "session_token": string}</pre>
400	<pre>{"error": "Petición mal formada", "session_token": string}</pre>
401	<pre>{"error": "OTP invalido o expirado", "session_token": string}</pre>
403	<pre>{"error": "session_token invalido o expirado" , "session_token": string}</pre>
413	<pre>{"files": [{"checksum_original": "SHA256", "status": "error"} "OK", "checksum_signed": "SHA256", "content": base 64}], "metadata": {"signed_failed": int, "OTP_expired": boolean, "files_signed": int, "files_received": int}, "session_token": string}</pre>
500	<pre>{"error": "Error Interno"}</pre>

Anexo A. Instalación aplicación móvil y configuración OTP

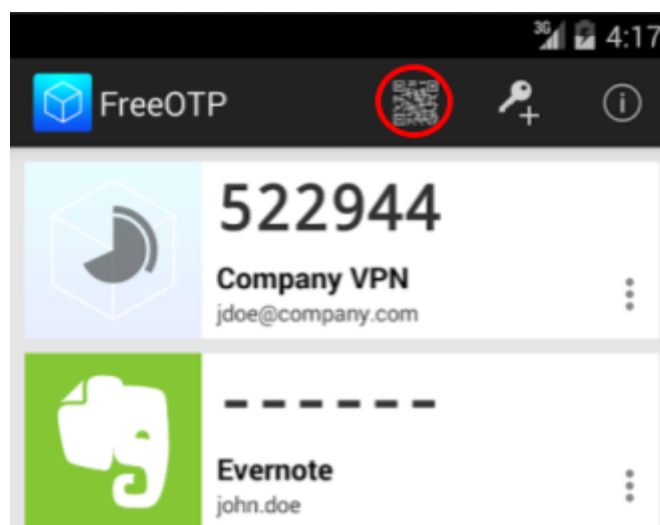
Es requisito habilitar una aplicación que permita generar un OTP válido al momento de realizar las pruebas al servicio. Por tal motivo, se ha habilitado una clave generadora de OTPs que permite utilizar un ambiente sandbox solo para la ejecución de pruebas.

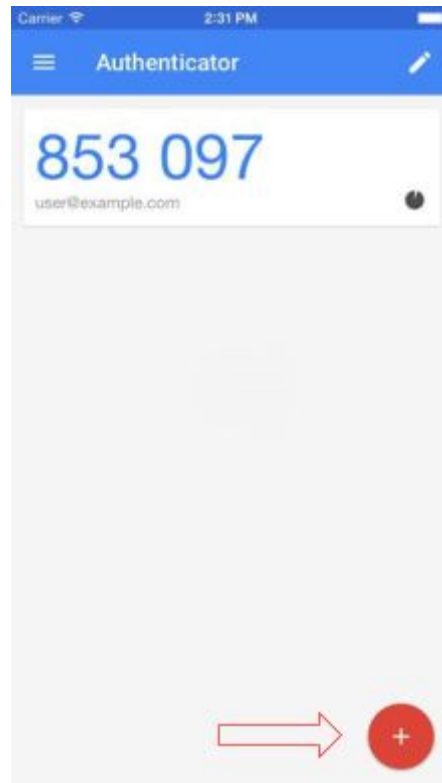
A continuación se detallan los pasos a seguir para habilitar un generador de OTP en un smartphone.

Aplicación OTP

Acceder a Google Play o App Store, descargar e instalar la aplicación **Free OTP** o **Google Authenticator** (para el ejemplo se ha utilizado un equipo con versión 5.1.1)

Abrir la aplicación ya instalada y habilitar la aplicación para la lectura de códigos QR.





Escanee el código QR.

Anexo B. Configuración para incrustar firma a PDF

Propiedad layout

La propiedad layout permite embeber una imagen asociada a la firma, análoga, de la persona que firma el documento electrónicamente. El siguiente XML muestra la estructura del layout.

```
<AgileSignerConfig>  
  <Application id="THIS-CONFIG">  
    <pdfPassword/>  
    <Signature>  
      <Visible active="true" layer2="false" label="true"
```

pos="\1\">

```

<llx></llx>
<lly></lly>
<urx></urx>
<ury></ury>
<page>LAST</page>
<image>BASE64</image>
<BASE64VALUE></BASE64VALUE>
</Visible>
</Signature>
</Application>
</AgileSignerConfig>

```

Variable	Descripción	Tipo Valor
llx	Coordenada x de la esquina inferior izquierda de la imagen.	Número entero
lly	Coordenada y de la esquina inferior izquierda de la imagen.	Número entero
urx	Coordenada x de la esquina superior derecha de la imagen.	Número entero
ury	Coordenada y de la esquina superior derecha de la imagen.	Número entero
page	Número de página donde se incluirá la imagen con la firma.	Numero entero. También es posible usar la palabra LAST para hacer referencia a la última hoja del documento.
image	Tipo de encoding utilizado para embeber la imagen	Texto. Valor constante a utilizar BASE64
base64value	Contenido de la imagen con el formato y encoding definido anteriormente.	Texto. Contenido del archivo en base64

Ejemplo:

Por restricciones de tamaño de archivo, el siguiente ejemplo no considera el contenido de la imagen. El ejemplo completo se encuentra publicado en [EjemploXmlLayout.xml](#)

```
<AgileSignerConfig>  
  <Application id="THIS-CONFIG">  
    <pdfPassword/>  
    <Signature  
      <Visible active="true" layer2="false" label="true"  
pos="1">  
      <llx>250</llx>  
      <lly>300</lly>  
      <urx>350</urx>  
      <ury>450</ury>  
      <page>LAST</page>  
      <image>BASE64</image>  
      <BASE64VALUE></BASE64VALUE>  
    </Visible>  
  </Signature>  
</Application>  
</AgileSignerConfig>
```

Anexo C. Definiciones y acrónimos

Acrónimo	Definición
API	Application Programming Interface
APP	Aplicación
JSON	JavaScript Object Notation
JWT	JSON Web Token
SHA256	hash criptográfico
OTP	One-Time Password
RA	Registration authority
XML	Extensible Markup Language

Término	Descripción
Firma atendida	Operación de firma en la cual se requiere la intervención del titular para la generación del OTP.
Firma desatendida	Operación de firma en la cual no se requiere la intervención del titular para la generación del OTP.

Anexo D. Historial de cambios

Versión	Fecha	Descripción
1	31/03/2016	Versión inicial
2	25/05/2016	Cambios menores de redacción e incorporación de códigos de error
3	15/09/2016	Cambios menores de redacción y ejemplos
4	15/11/2016	<ol style="list-style-type: none">1. Cambio estructura del documento2. Correcciones a parámetros en primera llamada3. Incorporación parámetros para firma XML y JSON4. Instalación y configuración aplicación iOS
5	31/01/2017	Cambio en código QR
6	24/03/2017	Cambios menores.
7	30/05/2017	Cambio en título de documento y corrección nombre de variables ejemplos firmas atendidas y desatendidas.
8	29/01/2020	Se modificó el documento de acuerdo a la nueva versión de API Se modificó el anexo A, configuración de OTP

Anexo E. Clasificación del documento

Este documento se encuentra clasificado bajo la categoría de ordinario, según el Instructivo de clasificación del Ministerio Secretaría General de la Presidencia.