



**Ministerio de Telecomunicaciones  
y de la Sociedad de la Información**

**SISTEMA FIRMAEC**

**Manual de Implementación Institucional**

**FirmaEC Descentralizada 2.1.0**

**Subsecretaría de Gobierno Electrónico**

11/10/2021  
Versión: 2.1.0

## HOJA DE CONTROL

### Información General

<b>Institución:</b>	Ministerio de Telecomunicaciones y de la Sociedad de la Información				
<b>Área:</b>	Dirección Nacional de Provisión de Servicios Electrónicos				
<b>Sistema:</b>	FirmaEC				
<b>Archivo:</b>	Manual de Implementación Institucional FirmaEC Descentralizada 2.1.0.odt				
<b>Elaborado:</b>	Misael Fernández				
<b>Revisado y Aprobado:</b>	Pablo Veintimilla				
<b>Versión/ Edición:</b>	2.1.0	<b>Número de páginas:</b>	27	<b>Fecha versión:</b>	11/10/2021

### Registro de cambios

Versión	Fecha	Autor	Descripción
1.0	25/09/2017	Misael Fernández	- Emisión Inicial.
1.1	27/09/2017	Pablo Veintimilla	- Correcciones de presentación.
1.2	03/10/2017	Misael Fernández	- Se agrega sección de pruebas al servicio web y otras correcciones.
1.3	13/10/2017	Misael Fernández	- Se agrega parámetros para usar el ambiente de preproducción y añade indicaciones para el envío de documentos para firmar.
1.4	16/10/2017	Pablo Veintimilla	- Correcciones de presentación.
1.5	18/10/2017	Misael Fernández	- Se eliminó servicios web que utiliza directamente la aplicación.
1.6	19/02/2018	Misael Fernández	- Se agrega la descripción de los parámetros y la respuesta que debe dar el servicio web del sistema requirente. - Se hace referencia a un archivo "rest" para evitar perder la consistencia en comandos al convertir en pdf.
1.7	13/09/2018	Misael Fernández	- Se agrega la descripción de los parámetros y se detalla mayor información para implementar servicios web SOAP. - Se hace referencia a nuevas herramientas para realizar pruebas de Servicios Web.
1.8	08/12/2018	Misael Fernández	- Se actualiza información del manual
1.9	13/08/2019	Misael Fernández	- Se actualiza información del manual
2.0	24/11/2020	María Jerez Misael Fernández Pablo Veintimilla	- Se incluye la descripción para la implementación de FirmaEC descentralizada
2.1.0	11/10/2021	Misael Fernández	- Actualizar marca gubernamental - Agregar información sobre el consumo del servicio web en REST al momento de devolver el

			documento firmado electrónicamente - Actualización de información al solicitar registro en ambiente de pruebas
--	--	--	--

## LICENCIA

República del Ecuador

Ministerio de Telecomunicaciones y de la Sociedad de la Información

Gobierno Electrónico

Manual de Implementación Institucional FirmaEC Descentralizada 2.1.0

Este documento se encuentra sujeto a la licencia

Creative Commons Atribución-No Comercial-Compartir Igual 4.0 Internacional



Usted es libre para:

- **Compartir** - copiar y redistribuir el material en cualquier medio o formato
- **Adaptar** - remezclar, transformar y crear a partir del material
- El licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

- **Atribución** - Usted debe darle crédito a esta obra de manera adecuada, proporcionando un enlace a la licencia, e indicando si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo del licenciante.
- **No Comercial** - Usted no puede hacer uso del material con fines comerciales.
- **Compartir Igual** - Si usted mezcla, transforma o crea nuevo material a partir de esta obra, usted podrá distribuir su contribución siempre que utilice la misma licencia que la obra original.
- **No hay restricciones adicionales** - Usted no puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otros hacer cualquier uso permitido por la licencia.

## CONTENIDO

1. Antecedentes.....	1
2. Introducción.....	4
3. Alcance.....	4
4. FirmaEC de Escritorio.....	5
4.1 Procedimiento para utilizar FirmaEC escritorio.....	6
5. FirmaEC Web Descentralizada.....	6
6. Procedimiento para la activación FirmaEC Descentralizada.....	8
7. Políticas para el Administrador Institucional de FirmaEC.....	8
8. Actores del sistema.....	9
9. Requisitos Técnicos.....	9
9.1 Hardware.....	9
9.2 Software.....	9
11. Proceso de firmado.....	11
11.1 Instalación del aplicativo FirmaEC en el equipo del usuario final.....	12
11.2 Invocación de servicio firma digital FirmaEC.....	12
11.3 Ejecución de la aplicación del lado del cliente.....	13
11.4 Respuesta de FirmaEC a sistema requirente.....	13
11.4.1 Servicio Web SOAP (deprecado).....	13
11.4.2 Servicio Web REST.....	14
12. Consumo servicio web REST de API (FirmaEC).....	17
12.1 Crear Documentos.....	17
12.2 Aplicación del lado del cliente.....	18
12.3 Especificación de protocolo.....	18
12.4 Especificación de parámetros.....	19
12.5 Utilización de JSON Web Token (JWT).....	20
13. Pruebas de Servicio Web REST.....	21
13.1 Navegador Firefox (Instalar Extensión RESTED).....	21
14. Pruebas de Servicio Web SOAP.....	22
14.1 Navegador Firefox (Instalar Extensión Wizdler).....	22
15. Glosario de términos.....	23

## 1. Antecedentes

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicado en el Registro Oficial Suplemento 557, de 17 de abril de 2002, en su última reforma, establece:

**Art. 14.- Efectos de la firma electrónica.-** "La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio."

**Art. 29.- Entidades de certificación de información.-** "Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República."

El Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, establece:

**Art. 132.- Adaptaciones necesarias para la utilización de software.-** Sin perjuicio de los derechos morales del autor, el titular de los derechos sobre el software, o el propietario u otro usuario legítimo de un ejemplar del software, podrá realizar las adaptaciones necesarias para la utilización del mismo, de acuerdo con sus necesidades, siempre que ello no implique su utilización con fines comerciales."

**Art. 147.- Acceso al código fuente.-** "Las entidades contratantes del sector público deberán poner a disposición del público, a través del sistema de Información de Ciencia, Tecnología, Innovación y Saberes Ancestrales, el código fuente del software de código abierto contratado o desarrollado. Se podrá mantener en reserva el código fuente del software contratado o desarrollado por instituciones públicas en los siguientes casos: a) Por razones de seguridad nacional; b) Por pertenecer a sectores estratégicos; y, c) Por considerarse por parte del ente de regulación en materia de gobierno electrónico la existencia de componentes críticos dentro del código, conforme la normativa vigente y lo que determine el reglamento de este código. En estos casos, en procura de salvaguardar el principio de transparencia y acceso, el código fuente de la versión inmediata anterior será accesible de forma restringida conforme las condiciones que el ente de regulación en materia de gobierno electrónico establezca para el efecto."

La Ley para la Optimización y Eficiencia de Trámites Administrativos, emitido el 16 de octubre de 2018, publicado en el Registro Oficial Suplemento 353 el 23 de octubre de 2018, establece:

**Art. 2.- Ámbito.-** "Las disposiciones de esta Ley son aplicables a todos los trámites administrativos que se gestionen en:

1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral, Transparencia y Control Social, en la Procuraduría General del Estado y la Corte Constitucional;
2. Las entidades que integran el régimen autónomo descentralizado y regímenes especiales;
3. Las empresas públicas;
4. Las entidades que tienen a su cargo la seguridad social;
5. Las entidades que comprenden el sector financiero público;

6. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado;

7. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados y regímenes especiales para la prestación de servicios públicos; y,

8. Las personas naturales o jurídicas del sector privado que sean gestoras delegadas o concesionarias de servicios públicos. Asimismo, el contenido de la presente Ley es aplicable a las relaciones que se generen a partir de la gestión de trámites administrativos entre el Estado y las y los administrados; entre las entidades que conforman el sector público; y entre éstas y las y los servidores públicos. Las disposiciones de esta Ley serán aplicables a las demás entidades del sector privado que tengan a su cargo trámites ciudadanos solo en los casos en que esta Ley lo establezca expresamente. Esta Ley no es aplicable a los trámites administrativos del sector defensa o que comprometan la seguridad nacional.”

El Decreto Ejecutivo No. 981, emitido el 28 de enero de 2020, publicado en el Registro Oficial 143 el 14 de febrero de 2020, establece:

**Art. 1.-** “Del gobierno electrónico.- La implementación del gobierno electrónico en la Función Ejecutiva, consiste en el uso de las tecnologías de la información y comunicación por parte de las entidades para transformar las relaciones con los ciudadanos, entre entidades de gobierno y empresas privadas a fin de mejorar la calidad de los servicios gubernamentales a los ciudadanos, promover la interacción con las empresas privadas, fortalecer la participación ciudadana a través del acceso a la información y servicios gubernamentales eficientes y eficaces y coadyuvar con la transparencia, participación y colaboración ciudadana.”

**Art. 2.-** “El Ministerio de Telecomunicaciones y de la Sociedad de la Información será la entidad rectora en gobierno electrónico de la Función Ejecutiva. Para la correcta implementación del gobierno electrónico ejercerá las siguientes atribuciones y responsabilidades: “3. Gestionar y coordinar la implementación de políticas, planes, programas y proyectos de gobierno electrónico en las instituciones de la Función Ejecutiva; (...) 5. Articular y coordinar con las demás instituciones de la Función Ejecutiva, así como con las otras Funciones del Estado y demás actores públicos y privados que directa o indirectamente coadyuven a la aplicación del presente Decreto; (...)”; y, en su artículo 4, establece: “(...)b. Utilizar los medios electrónicos que determine el Ministerio de Telecomunicaciones y de la Sociedad de la Información, para la aplicación efectiva de las políticas de gobierno electrónico en la gestión pública.(...)”

**Disposición General Segunda.-** Las autoridades, funcionarios y servidores públicos que en el ejercicio de sus funciones suscriban documentos, deberán contar obligatoriamente, a su costo, con un certificado de firma electrónica para persona natural válido de acuerdo con la normativa que el Ministerio de Telecomunicaciones y de la Sociedad de la Información emita para el efecto. Todo documento que atribuya responsabilidad de elaboración, revisión, aprobación, emisión y/o certificación, deberá ser firmado electrónicamente. Las autoridades, funcionarios y servidores públicos que se nieguen a aceptar documentos firmados electrónicamente, validados en el sistema oficial, serán sancionados conforme a la normativa vigente.



El Acuerdo Ministerial No. 005-2020, del 17 de febrero de 2020, dispone:

**Art. 2.-** *“Delegar al funcionario nombrado como Subsecretario de Estado (Gobierno Electrónico), para que a nombre y representación del señor Ministro de Telecomunicaciones y de la Sociedad de la Información, ejerza las siguientes atribuciones:*

a) *Regular, planificar, coordinar, controlar, realizar el seguimiento y gestionar las acciones orientadas a la simplificación, optimización y eficiencias de trámites administrativos de las instituciones del sector público, a fin de reducir la complejidad administrativa y los costos relacionados con dichos trámites, de acuerdo a la Ley Orgánica de Optimización de Trámites Administrativos (...)*

f) *Suscribir las actas de entrega – recepción entre el Ministerio de Telecomunicaciones y de la Sociedad de la Información y entidades del sector público y privado para aplicativos de software de código abierto que estén bajo la responsabilidad del MINTEL(...)*”

El Acuerdo Ministerial No. 017-2020, publicado en el Registro Oficial N° 244 del 13 de julio de 2020, establece:

**Art. 5.- “Sistema oficial de validación de documentos firmados electrónicamente.-** *El sistema oficial para validación de documentos firmados electrónicamente será el sistema FirmaEC, provisto por el Ministerio de Telecomunicaciones y de la Sociedad de la Información. En caso de que alguna entidad posea un sistema implementado para el efecto, podrá continuar con su uso mientras sea compatible con todos los certificados de firma emitidos por las entidades autorizadas por la Agencia de Regulación y Control de las Telecomunicaciones y cumplan con los estándares establecidos. El Ministerio de Telecomunicaciones y de la Sociedad de la Información pondrá a disposición de las entidades la aplicación FirmaEC, así como su código fuente liberado con licencia de software libre, a fin de que las instituciones puedan adecuar sus procedimientos y sistemas informáticos en caso de requerirlos.”*

El Acuerdo Nro. SENESCYT-2019-111, establece:

**Art. 1.-** *Establece a la plataforma digital MINKA como repositorio y plataforma colaborativa de desarrollo de software libre y de código abierto.*

**Art. 2.-** *Incorpórese a la plataforma digital MINKA como componente integrante del Sistema Nacional de Información de Ciencia, Tecnología, Innovación y Conocimientos Tradicionales.*

**Art. 3.-** *La plataforma digital MINKA deberá incluir todos los artefactos, sean estos manuales técnicos o de usuario, componentes, librerías, del software libre y de código abierto desarrollado o adquirido a título gratuito u oneroso, por las entidades del sector público, especificando su tipo de licencia, que según la normativa vigente deben ser puestos a disposición del público a través del Sistema Nacional de Información de Ciencia, Tecnología, Innovación y Conocimientos Tradicionales, de acuerdo a los lineamientos establecidos por el ente regulador de gobierno electrónico.*

**Art. 4.-** *La Secretaría de Educación Superior, Ciencia, Tecnología e Innovación a través de la Coordinación General de Tecnologías de la Información y Comunicación garantizará la disponibilidad de la plataforma digital MINKA, mediante el alojamiento, mantenimiento, actualización y soporte técnico a la infraestructura tecnológica de dicha plataforma, para lo cual deberá encargarse de la gestión operativa y financiera de la misma. Así mismo, deberá definir y*

crear en la plataforma digital MINKA ambientes específicos diferenciados que estarán bajo la gestión exclusiva de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación.

## 2. Introducción

FirmaEC es un conjunto de aplicaciones informáticas que permiten firmar y verificar documentos electrónicos; también permite validar certificados digitales en archivo o token emitidos por entidades certificadoras acreditadas por la ARCOTEL. Puede ser utilizado como un aplicativo de escritorio o como un componente web.

Su aplicativo de escritorio es compatible con los sistemas operativos Windows, Linux y Mac.

Su aplicativo web permite procesar firma(s) electrónica(s) de manera sencilla para el usuario, firmando documentos digitales con extensiones PDF o XML con los navegadores existentes en el mercado como Mozilla Firefox, Google Chrome, Safari, Edge, entre otros.

FirmaEC, posee los siguientes componentes:

- **Aplicativo de escritorio:** permite firmar y verificar documentos electrónicos; también permite validar certificados digitales. Los documentos son generados directamente por el usuario. Es compatible con los sistemas operativos Windows, Linux y Mac.
- **Web:** permite procesar firma electrónica de manera sencilla para el usuario, firmando documentos digitales a través de navegadores como Mozilla Firefox, Google Chrome, Safari, Edge entre otros. Los documentos a ser firmados son generados través de sistemas web accesibles mediante internet. El componente web trabaja en 2 modalidades:
  - o **Centralizado:** mediante un servidor administrado y provisto por el MINTEL, se procesan solicitudes de firma y verificación de documentos. Esta modalidad utiliza infraestructura del MINTEL.
  - o **Descentralizado:** mediante servidores administrados o provistos por terceros, se procesan solicitudes de firma y verificación de documentos. Esta modalidad utiliza infraestructura de terceros.

## 3. Alcance

El presente documento es la guía necesaria para que el Administrador Institucional de FirmaEC realice la implementación del aplicativo en su Institución Pública o Privada, para posteriormente solicitar la autorización de usar el software oficial FirmaEC brindada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL).

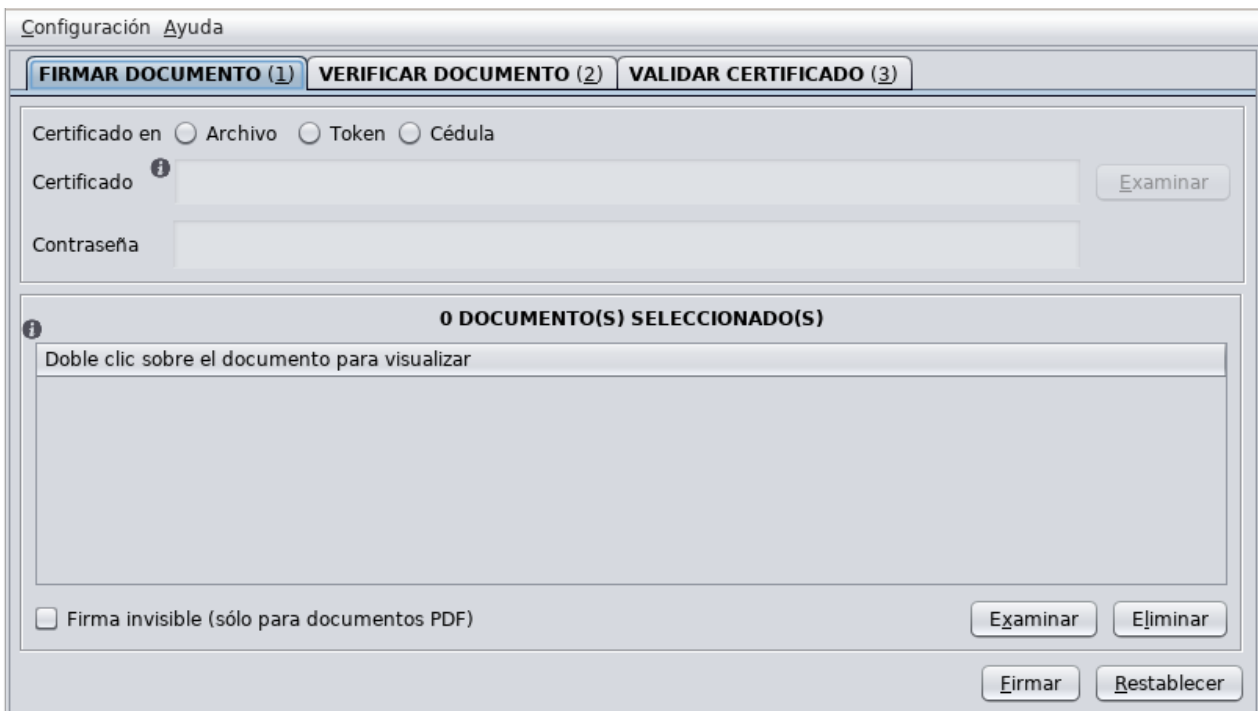
La utilización de FirmaEC, sus servicios o componentes implica la aceptación plena y sin reservas de todas las disposiciones contenidas en **Acuerdo de Términos y Condiciones de Uso** publicado en el portal <https://www.firmadigital.gob.ec/acuerdo-de-uso>



En virtud que los Términos pueden ser modificados en cualquier momento por MINTEL, se recomienda su atenta lectura en cada una de las ocasiones en que se proponga utilizar FirmaEC.

Las nuevas versiones entrarán en vigor a partir del momento de su publicación en el portal <https://www.firmadigital.gob.ec/>

#### 4. FirmaEC de Escritorio



The screenshot shows the 'FirmaEC de Escritorio' application window. At the top, there are tabs for 'FIRMAR DOCUMENTO (1)', 'VERIFICAR DOCUMENTO (2)', and 'VALIDAR CERTIFICADO (3)'. Below the tabs, there are radio buttons for 'Certificado en' with options: Archivo, Token, and Cédula. There are input fields for 'Certificado' and 'Contraseña', with an 'Examinar' button next to the 'Certificado' field. Below this, a section titled '0 DOCUMENTO(S) SELECCIONADO(S)' contains a large empty area with the instruction 'Doble clic sobre el documento para visualizar'. At the bottom, there is a checkbox for 'Firma invisible (sólo para documentos PDF)' and buttons for 'Examinar', 'Eliminar', 'Firmar', and 'Restablecer'.

Software ejecutado en el computador de cada usuario mediante el cual se realiza el proceso de firmado de documentos. Esta aplicación permite cumplir el principio de no repudio e integridad pues garantiza que el documento a firmar esté en custodia del firmante

#### 4.1 Procedimiento para utilizar FirmaEC escritorio

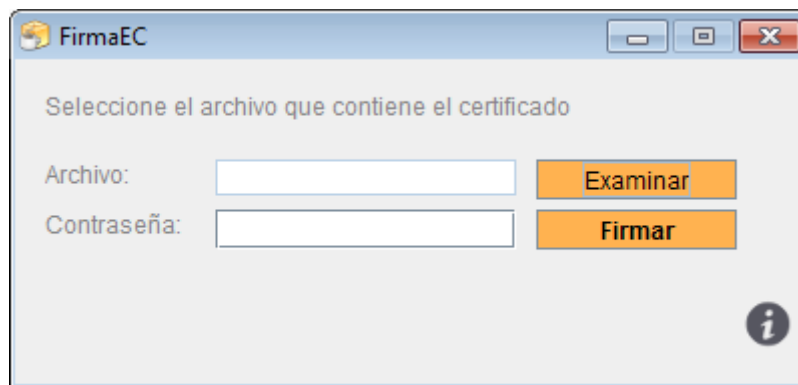
1. Descarga e Instalar FirmaEC, el instalador se encuentra en sitio web oficial <https://www.firmadigital.gob.ec> en la sección “**Enlaces rápidos**” y se deberá descargar el instalador dependiendo el sistema operativo que corresponda.

2. Una vez finaliza la instalación aparecerá en su escritorio el siguiente icono:



3. Una vez instalado el usuario podrá firmar electrónicamente y verificar documentos y certificados. Cabe señalar que para firma electrónicamente previamente deberá obtener certificado digital emitido por las entidades certificadoras autorizadas por la ARCOTEL.

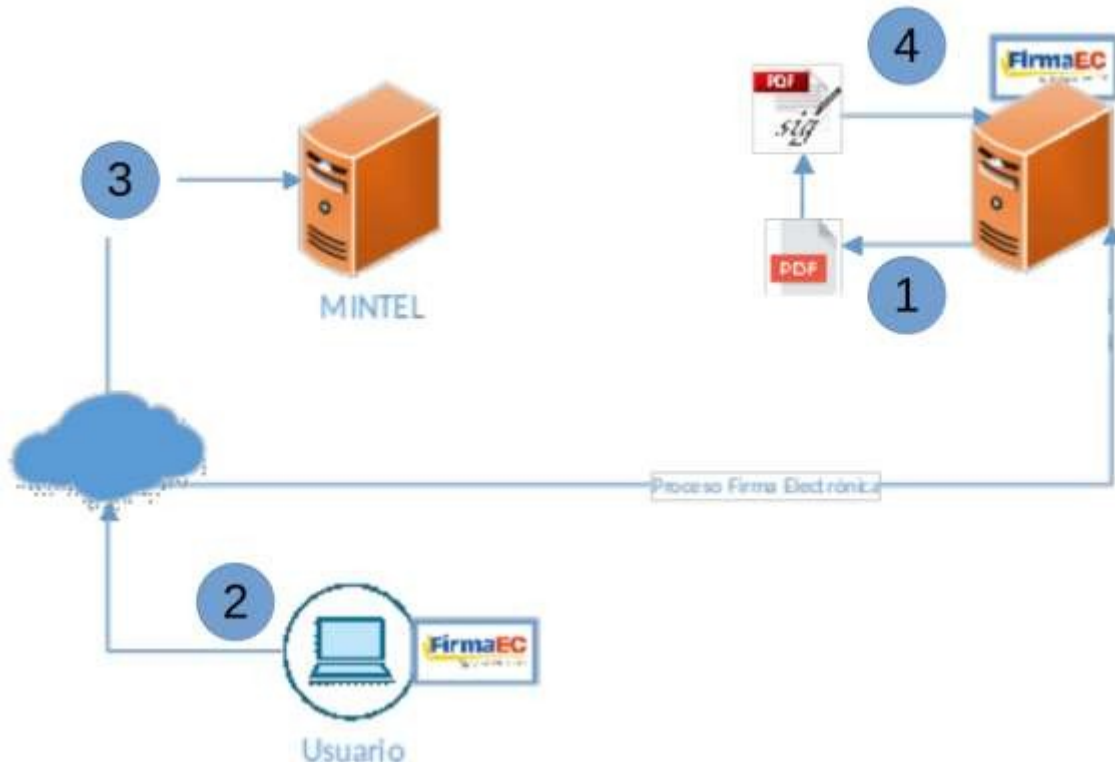
#### 5. FirmaEC Web Descentralizada



FirmaEC Web Descentralizada permite utilizar los servicios de firma electrónica en infraestructura propia

Se encuentra disponible para los sistemas requirentes de las Instituciones Públicas o Privadas que requieran implementar el proceso de firma electrónica para simplificar sus procesos y requiere la autorización por MINTEL para usar el software oficial FirmaEC.

Su funcionamiento es descrito en la siguiente figura:



1. Un sistema web de una institución pública o privada, genera un(os) documento(s) que requiere(n) ser firmado(s) y estos son enviados a los servidores de FirmaEC instalados en la infraestructura de terceros.

2. Los documentos son enviados al usuario en su computador, quien mediante FirmaEC Web, firma el documento.

3. FirmaEC Web previo a devolver el documento firmado, consulta si el servidor de FirmaEC instalado en infraestructura de terceros ha sido registrado y autorizado por MINTEL. En caso de no estar registrado una advertencia proveyendo un potencial riesgo de seguridad, consultando al usuario si desea consultar.



4. Los documentos firmados automáticamente son enviados a los servidores de FirmaEC instalados en la infraestructura de terceros.

## 6. Procedimiento para la activación FirmaEC Descentralizada

1. Aceptar plenamente y sin reservas de todas las disposiciones contenidas en Acuerdo de Términos y Condiciones de Uso publicado en el portal <https://www.firmadigital.gob.ec/acuerdo-de-uso>
2. Instalar los componentes de FirmaEC Descentralizada en la infraestructura del solicitante, para ello se deberá compilar el proyecto [firmadigital-api](#) y el proyecto [firmadigital-servicio](#). Deberá cumplir con los criterios de seguridad y uso definidos en los términos de uso.
3. Adecuar el sistema web que generará el documento a firmar, mediante la exposición de un servicio web que será utilizado para devolver el documento firmado electrónicamente.
4. Desarrollar lo establecido en la sección **11.4 Respuesta de FirmaEC a sistema requirente**
5. Una vez completadas satisfactoriamente las pruebas, solicitar mediante correo electrónico dirigido a [servicios@gobiernoelectronico.gob.ec](mailto:servicios@gobiernoelectronico.gob.ec), adjuntando el oficio firmado por la máxima autoridad o su delegado, en el que indica el URL del servicio web API del sistema requirente, informe de pruebas realizadas a entera satisfacción y la delegación del Administrador Institucional de FirmaEC, con la siguiente información:
  - Nombres y Apellidos completos
  - Correo Electrónico institucional
  - Número de teléfono de contacto

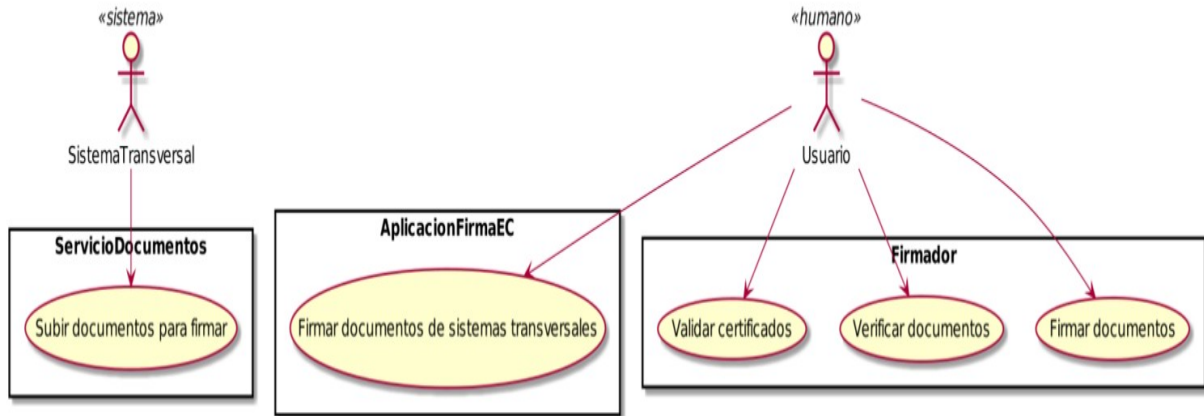
El AIF es la persona responsable y contacto técnico para la implementación del servicio FirmaEC.

6. MINTEL procederá a registrar el servidor del solicitante, siempre y cuando cumpla con los criterios de seguridad (uso de SSL y publicación a través del subdominio)

## 7. Políticas para el Administrador Institucional de FirmaEC

- El Administrador Institucional de FirmaEC (AIF) es delegado por la máxima autoridad de la Institución o su delegado, por medio de un oficio enviado a la autoridad de la Subsecretaría de Gobierno Electrónico y Registro Civil.
- El AIF es la persona que se va a encargar de la gestión de la implementación del servicio FirmaEC.
- El AIF es el encargado de brindar soporte a los usuarios que utilicen el servicio de FirmaEC y será el único contacto con Gobierno Electrónico.

## 8. Actores del sistema



Existen dos tipos de Actores en el sistema:

- **SistemaTransversal:** Es el sistema requirente que inicia el proceso de firma digital al subir los documentos a firmar al sistema, mediante el ServicioDocumentos.
- **Usuario:** Es la persona que utiliza uno de los dos programas desarrollados:
  - **Cliente:** Es la aplicación Java para la firma de documentos creados por el sistema requirente.
  - **Firmador:** Es la aplicación Java para la firma de cualquier tipo de documento provisto por el usuario. Adicionalmente permite verificar documentos firmados y validar certificados digitales.

## 9. Requisitos Técnicos

Es interés del Gobierno ecuatoriano alcanzar soberanía y autonomía tecnológica, así como un ahorro de recursos públicos, para lo cual se recomienda levantar una infraestructura con las siguientes características:

### 9.1 Hardware

<b>Procesador</b>	4 CPU's
<b>Disco Duro</b>	30 Gb
<b>Memoria RAM</b>	4 Gb

### 9.2 Software

<b>Sistema Operativo</b>	Centos 8 (modo consola)
<b>Servicio Web</b>	WildFly 20
<b>Máquina Virtual</b>	OpenJDK 11
<b>Base de Datos</b>	PostgreSQL 12

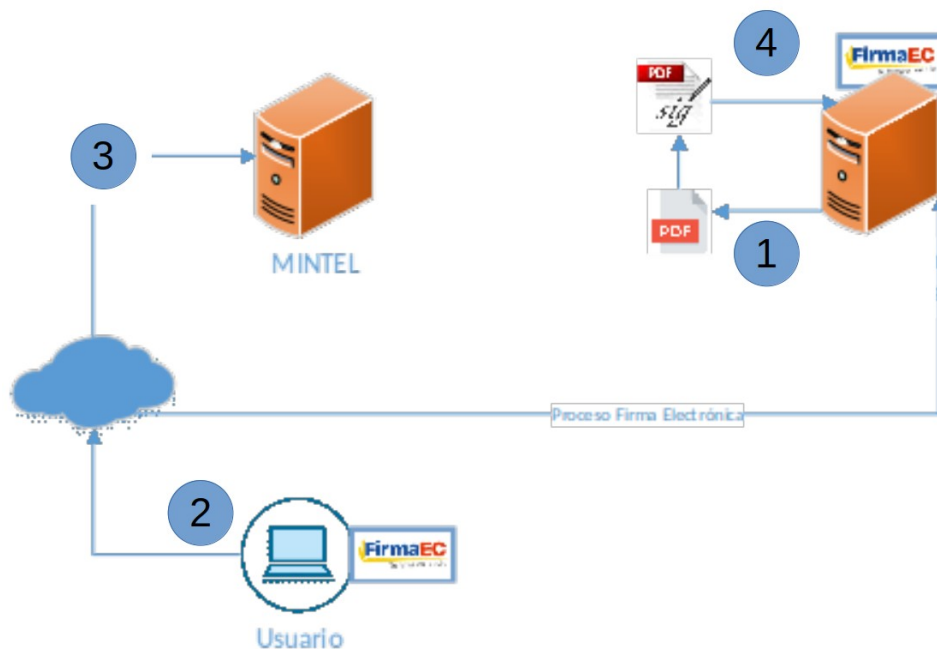
Para que el servicio funcione se requiere implementar los componentes:

- [firmadigital-api](#) (revisar README del proyecto).
- [firmadigital-servicio](#) (revisar README del proyecto).
- Base de datos.

Adicionalmente se necesita tener conocimientos en:

- Desarrollo java.
- Administración de servidores.
- Administración de servicios Web.
- Administración de Base de Datos.

## 10. Proceso de firmado descentralizada



FirmaEC se encuentra disponible para los sistemas requirentes de la Función Ejecutiva que requieran implementar el proceso de firma electrónica para simplificar los trámites en línea.

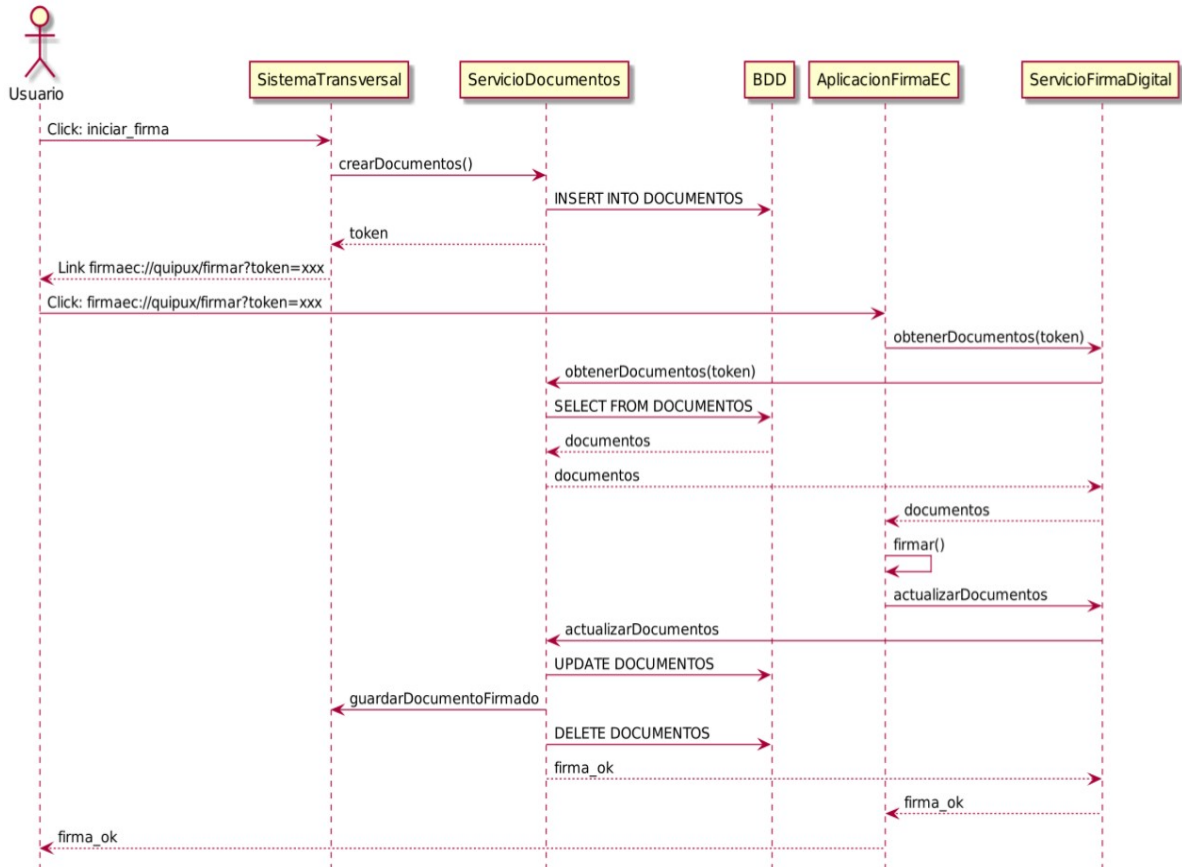
Para iniciar el proceso de firma electrónica, el usuario debe tener instalado la aplicación de escritorio FirmaEC en su equipo, al momento de abrir dicho aplicativo se establece la comunicación con los servidores de MINTEL y accede al documento a firmar.

En este paso se realiza la validación del certificado digital para firmar el documento en extensión PDF o XML, con la fecha y hora obtenida de los servidores de MINTEL.

Terminado el proceso, el documento firmado retorna al sistema requirente.



## 11. Proceso de firmado



Previamente, debe estar deployado los compilados de los proyectos [firmadigital-api](#) y [firmadigital-servicio](#) en la infraestructura de la institución requirente.

El proceso de firma digital se inicia desde el lado de un sistema requirente, que solicita se firme uno o varios documentos.

Se invoca un servicio web (REST) en la aplicación ServicioDocumentos, para que se inicie el proceso de firma digital. Esta aplicación recibe uno o varios documentos en un formato JSON. El servicio retorna un token en formato JSON Web Tokens o JWT para continuar con el proceso.

Una vez obtenido el token JWT después de invocar el servicio de creación de documentos, el sistema requirente es el responsable de presentar al usuario en interface un link o botón para invocar el proceso de firma del lado del cliente.

Para esto se ha ideado un protocolo **firmaec://** que está relacionado a un programa desarrollado en Java que se debe instalar previamente en cada cliente. Mediante un Protocol Handler en el sistema operativo se configura que todos los links en el navegador que inicien con el protocolo **firmaec://** sean abiertos con esta aplicación.

Esto permite efectivamente ejecutar lógica en forma externa al navegador web, pero invocada por un link en la interface del sistema requirente. Una vez abierta la aplicación del lado del cliente se

solicita el certificado PKCS#12 en archivo o en token USB de firma digital y se procede con la firma.

Los documentos firmados por la aplicación son enviados hacia el servicio ServicioFirmaDigital, el mismo que delega en el ServicioDocumento que almacena los documentos firmados en la base de datos. Los documentos firmados son recibidos y almacenados temporalmente en una base de datos. Luego son enviados de vuelta al sistema requirente mediante la invocación de un servicio Web REST o SOAP, configurado por cada sistema.

### 11.1 Instalación del aplicativo FirmaEC en el equipo del usuario final

Para usar FirmaEC, el usuario final debe descargar desde el link: <https://www.firmadigital.gob.ec/descargar-firmaec/> el instalador dependiendo del sistema operativo y arquitectura del equipo.

Este instalador permite firmar documentos desde el sistema requirente, firmar documentos locales, verificar documentos firmados y validar certificados digitales.

### 11.2 Invocación de servicio firma digital FirmaEC

El proceso de firma digital se inicia desde el lado de un sistema requirente, que solicita se firme uno o varios documentos invocando al servicio web (REST) correspondiente **12. Consumo servicio web REST de API (FirmaEC)**, consumiendo el servicio web del proyecto [firmadigital-servicio](#), previamente modificado, compilado y publicado en su infraestructura..

Este servicio web recibe uno o varios documentos en un formato JSON como este:

```
{
  "sistema": "pruebas",
  "cedula": "171057635",
  "documentos": [
    {
      "nombre": "documento1.pdf"
      "documento": "JVBERi0xLjQKJc0kw7zDts0fCjIgMC3RoIDMgMCBSL..."
    },
    {
      "nombre": "documento2.pdf"
      "documento": "JVBERi0xLjQKJc0kw7zDts0fCjIgMC3RoIDMgMCBSL..."
    }
  ]
}
```

El servicio retorna un token en formato JSON Web Tokens o JWT para continuar con el proceso.

**Nota:** El servicio FirmaEC, no estampa de manera visible la firma digital en el documento, por lo que si se desea una marca de la firma en el documento que indique su estado firmado, lo debe generar antes de enviar el sistema requirente.

### 11.3 Ejecución de la aplicación del lado del cliente

Una vez obtenido el token JWT después de invocar el servicio de creación de documentos, el sistema requirente es el responsable de presentar al usuario en interface un link o boton para invocar el proceso de firma del lado del cliente.

Para esto se ha ideado un protocolo **firmaec://** mismo que será atendido por el software instalado en el paso **11.1 Instalación del aplicativo FirmaEC en el equipo del usuario final** Mediante un Protocol Handler en el sistema operativo se configura que todos los links en el navegador que inicien con el protocolo **firmaec://** sean abiertos con esta aplicación. Esto permite efectivamente ejecutar lógica en forma externa al navegador web, pero invocada por un link en la interface del sistema requirente.

Una vez el usuario de clic en el link, en la aplicación del lado del cliente solicita el certificado PKCS#12 en archivo o un token USB de firma digital y se procede con la firma.

Debido a que solamente el usuario tiene bajo su posesión el certificado digital o token USB utilizados para el proceso de firma por razones de seguridad **FirmaEC no almacena los certificados de usuario.**

### 11.4 Respuesta de FirmaEC a sistema requirente

El sistema que implementa FirmaEC, debe tener publicado un servicio web REST o SOAP, el cual recibe el documento firmado y devolver una respuesta de confirmación.

#### 11.4.1 Servicio Web SOAP (deprecado)

Una vez FirmaEC recibe el documento, este invoca automática al servicio web SOAP registrado por el sistema requirente enviado de vuelta el documento firmado digitalmente.

Para levantar el sistema que implementará la firma electrónica deberá tener un Servicio Web publicado a través del puerto **443** con estilo **RPC**, con la definición de **name="soapapiorfeo"** y **targetNamespace="urn:soapapiorfeo"** publicado y listo para consumir, de esta forma se retornará el documento firmado.

El Servicio Web debe recibir la siguiente información por medio de una acción llamada obligatoriamente **"grabar\_archivos\_firmados"**:

El WSDL devuelto sigue el siguiente formato:

Parámetro	Tipo	Opcional	Descripción
set_var_usuario	String	No	Cédula de identidad del usuario
set_var_documento	String	No	Nombre del documento firmado
set_var_archivo	base64Binary	No	Contenido del documento firmado, en formato Base 64.
set_var_datos_firmante	String	No	Nombres y Apellidos del firmante
set_var_fecha	String	No	Fecha que se firmó el documento <b>formato ISO-8601 (2019-01-17T03:51:28-05:00)</b>
set_var_institucion	String	Si	Institución del firmante
set_var_cargo	String	Si	Cargo del firmante

**Respuesta** (name="result" type="string")

Valor (String)	Descripción
1	Se recibió el documento
0	No se recibió el documento

**ADVERTENCIA:**

Se debe realizar el control previo de los documentos recibidos por el servicio web.

**11.4.2 Servicio Web REST**

Una vez FirmaEC recibe el documento, este invoca automática al servicio web REST registrado por el sistema requirente enviado de vuelta el documento firmado digitalmente.

Para levantar el sistema que implementará la firma electrónica deberá tener un Servicio Web publicado y listo para consumir a través del puerto **443** con **subdominio**, de esta forma se retornará el documento firmado.

El Servicio Web debe recibir la siguiente información por medio de una acción llamada obligatoriamente "**grabar\_archivos\_firmados**":

Consumes	Produce
application/json	application/text

**Parámetros Header**

Se debe incluir como Header el parámetro *X-API-KEY* con un API KEY provisto para FirmaEC.

Parámetro	Tipo	Opcional	Descripción
X-API-KEY	String	No	API Key del Sistema FirmaEC ( <b>no SHA256</b> )

**Parámetros Body**

Parámetro	Tipo	Opcional	Descripción
cedula	String	No	Cédula de identidad del usuario del sistema
nombreDocumento	String	No	Nombre del documento firmado
archivo	String	No	Contenido del documento firmado, en formato Base 64.
firmasValidas	Boolean	No	Validación final de todos los certificados digitales con el que se realizó el proceso de firmado
integridadDocumento	Boolean	No	Validación final de la integridad del documentos (firma digital cubre todo el documento)
error	String	Si	Mensaje de error, en caso de existir

<b>Lista de Objetos tipo Certificado</b>			
Contiene la información de una o varias firmas del documento			
emitidoPara	String	No	Nombre y apellido del firmante
emitidoPor	String	No	Entidad certificadora que emitió el certificado digital
validoDesde	String	No	Fecha que se emitió el certificado digital <b>formato ISO-8601</b> <b>(2019-01-17T03:51:28-05:00)</b>
validoHasta	String	No	Fecha que caducó el certificado digital <b>formato ISO-8601</b> <b>(2019-01-17T03:51:28-05:00)</b>
fechaFirma	String	No	Fecha que se firmó el documento <b>formato ISO-8601</b> <b>(2019-01-17T03:51:28-05:00)</b>
fechaRevocado	String	Si	Fecha que se revocó el certificado digital <b>formato ISO-8601</b> <b>(2019-01-17T03:51:28-05:00)</b>
certificadoVigente		No	Validación de la vigencia del certificado digital
clavesUso	String	No	El propósito por el que fue emitido el certificado digital:Firma Electrónica, No Repudio, Cifrado de llave, Cifrado de datos, Acuerdo de llaves, Firma y certificado de llave, Firma de CRL, Solo cifrado, Solo descifrado
fechaSelloTiempo	String	Si	Fecha que realizó el sello de tiempo <b>formato ISO-8601</b> <b>(2019-01-17T03:51:28-05:00)</b>
integridadFirma	Boolean	No	Validación de la integridad del certificado digital con el que se realizó el proceso de firmado
razonFirma	String	Si	Motivo por el cual se firma el documento
localizacion	String	Si	Localización (Institución, área, ciudad, etc) del documento
cedula	String	No	Cédula de identidad del firmante
nombre	String	No	Nombres del firmante
apellido	String	No	Apellidos del firmante
institucion	String	Si	Institución del firmante
cargo	String	Si	Cargo del firmante
entidadCertificadora	String	No	Entidad certificadora que emitió el certificado digital
serial	String	No	Código serial del certificado digital
selladoTiempo	Boolean	Si	Estado que indica el sellado de tiempo
certificadoDigitalValido	Boolean	No	Validación de la emisión del certificado digital con el que se realizó el proceso de firmado

### Ejemplo JSON de retorno al sistema requirente

```
{
  "cedula": "0704604032",
  "nombreDocumento": "nombreDocumento.pdf",
  "archivo": "JVBERi0xLjQKJc0kw7zDtsOfCjIgMC3RoIDMgMCBSL...",
  "firmasValidas": true,
  "integridadDocumento": true,
  "error": "null",
  "certificado": [
    {
      "emitidoPara": "MISAEI VLADIMIR FERNANDEZ CORREA",
      "emitidoPor": "Anf AC",
      "validoDesde": "",
      "validoHasta": "",
      "fechaFirma": "",
      "fechaRevocado": "",
      "certificadoVigente": true,
      "clavesUso": "",
      "fechaSelloTiempo": "",
      "integridadFirma": true,
      "razonFirma": "Firma de responsabilidad",
      "localizacion": "Subsecretaría de Gobierno Electrónico",
      "cedula": "0704604032",
      "nombre": "MISAEI VLADIMIR",
      "apellido": "FERNANDEZ CORREA",
      "institucion": "MINTEL",
      "cargo": "Especilista",
      "entidadCertificadora": "Anf AC",
      "serial": "0123456789",
      "selladoTiempo": false,
      "certificadoDigitalValido": true
    },
    {
      "emitidoPara": "MISAEI VLADIMIR FERNANDEZ CORREA",
      "emitidoPor": "Anf AC",
      "validoDesde": "",
      "validoHasta": "",
      "fechaFirma": "",
      "fechaRevocado": "",
      "certificadoVigente": true,
      "clavesUso": "",
      "fechaSelloTiempo": "",
      "integridadFirma": true,
      "razonFirma": "Firma de responsabilidad",
      "localizacion": "Subsecretaría de Gobierno Electrónico",
      "cedula": "0704604032",
      "nombre": "MISAEI VLADIMIR",
      "apellido": "FERNANDEZ CORREA",
      "institucion": "MINTEL",
      "cargo": "Especilista",
      "entidadCertificadora": "Anf AC",
      "serial": "0123456789",
      "selladoTiempo": false,
      "certificadoDigitalValido": true
    }
  ]
}
```



## Respuesta

Valor (String)	Descripción
OK	Se recibió el documento

### ADVERTENCIA:

Se debe realizar el control previo de los documentos recibidos por el servicio web.

## 12. Consumo servicio web REST de API (FirmaEC)

Para el desarrollo de la funcionalidad de firma digital utilizada por el sistema requirente, se ha definido los siguientes servicios REST que confirman un API, consumiendo el servicio web del proyecto [firmadigital-servicio](#), previamente modificado, compilado y publicado en su infraestructura.

### 12.1 Crear Documentos

Crea uno o varios documentos para ser firmados por la aplicación del lado del cliente.

POST /servicio/documentos

### Produce

application/text

### Parámetros Header

Se debe incluir como Header el parámetro *X-API-KEY* con un API KEY provisto para cada sistema requirente.

Parámetro	Tipo	Opcional	Descripción
X-API-KEY	String	No	API Key del Sistema Requirente ( <b>no SHA256</b> )

### Parámetros Body

Parámetro	Tipo	Opcional	Descripción
sistema	String	No	Sistema requirente registrado por FirmaEC
cedula	String	No	Cédula de identidad del usuario
documentos	Array	No	Arreglo de documentos, con parámetros "nombre" y "documento"
nombre	String	No	Nombre del documento a firmar
documento	String	No	Contenido del documento a firmar, en formato Base 64

## Respuesta

HTTP Code	Descripción
201	Operación exitosa
400	Error al decodificar JSON, no se cumple el schema
403	Error al validar el API Key

## Ejemplo JSON de retorno al sistema requirente

```
{
  "sistema": "pruebas",
  "cedula": "171057635",
  "documentos": [
    {
      "nombre": "documento1.pdf"
      "documento": "JVBERi0xLjQKJc0kw7zDts0fCjIgMC3RoIDMgMCBSL..."
    },
    {
      "nombre": "documento2.pdf"
      "documento": "JVBERi0xLjQKJc0kw7zDts0fCjIgMC3RoIDMgMCBSL..."
    }
  ]
}
```

**NOTA:** Se puede enviar uno o varios documentos, considerando que el JSON generado contenga en el campo **documentos**, un objeto o lista de objetos con todos el(los) documento(s) a firmar.

## 12.2 Aplicación del lado del cliente

Esta aplicación es invocada mediante un link (generar hipervínculo) en una página web del sistema requirente, que tiene un protocolo especial, registrado en el sistema operativo del usuario.

## 12.3 Especificación de protocolo

El protocolo FirmaEC está formado por los siguientes componentes:

*firmaec://sistema/accion?parámetro1=valor1&parámetro2=valor2&parámetro3=valor3...*

- **sistema:** El sistema requirente que solicita la firma digital (X-API-KEY)
- **accion:** Determina la acción a ejecutar en la aplicación, puede ser:
- **firmar:** Para proceder a la firma de un documento
- **parámetro:** permite enviar parámetro con un valor a la aplicación

**NOTA:** Para enviar los parámetros, se debe codificar estilo URL de acuerdo al RFC 3986.

Debemos codificar la variable que tiene caracteres conflictivos a formato URL. En PHP utilizamos la función `rawurlencode()`, que viene en la librería de funciones.

Este link debe ser construido del lado del servidor, y presentado en la aplicación web.

## 12.4 Especificación de parámetros

Los parámetros se encuentran detallados a continuación:

Parámetro	Tipo	Opcional	Descripción
token	String	No	JWT devuelto por el servicio web de FirmaEC
tipo_certificado	Integer	Si (desde versión 2.10.0)	<b>1</b> =Token <b>2</b> =Archivo <b>3</b> =Tarjeta inteligente (cédula)
format	String	Si	<b>xml</b> =Documento en formato xml (esta opción no permite estampar firma)
llx	Integer	Si	En formato A4 Posición X (positionOnPageLowerLeftX)
lly	Integer	Si	En formato A4 Posición Y (positionOnPageLowerLeftY)
urx	Integer	Si	En formato A4 Posición X (positionOnPageUpperRightX)
ury	Integer	Si	En formato A4 Posición Y (positionOnPageUpperRightY)
estampado	String	Si	<b>QR</b> =Información estampada en QR <b>information1</b> =Información personalizada <b>information2</b> =Información con estándar ETSI TS 102 778-6 V1.1.1
razon	String	Si	Razón por la cual se firma el documento (ejemplo: "firmado desde https://sistema.requirente.gob.ec")
pagina	Integer	Si	Página en la que se estampará la firma digital (si no se establece el parámetro, por defecto es la última página)
pre	Boolean	Si	<b>true</b> =Hace referencia al ambiente de pruebas

### Ejemplos:

Se debe generar hipervínculo con lo siguiente:

#### PDF

`firmaec://pruebas/firmar?  
token=1232434343&tipo_certificado=2&llx=222&lly=85&estampado=QR&razon=firmaEC&pre=true`

#### XML

`firmaec://pruebas/firmar?token=1232434343&tipo_certificado=2&format=xml&pre=true`

## 12.5 Utilización de JSON Web Token (JWT)

El token retornado por FirmaEC, esta basado en el token JWT que implementa el estándar descrito en <https://jwt.io> (Revisar información sobre codificar, decodificar y el uso e implementación de la librería), y permite mantener la integridad al intercambiar parámetros entre el cliente y el servidor. Este token está formado por 3 componentes, separados por un "." (punto) y codificados en Base 64.

Por ejemplo (puede codificar o decodificar desde <https://jwt.io>):

```
eyJhbGciOiJIUzI1NiJ9.eyJzZWR1bGEiOiIxMjM0NTY3ODIsInNpc3RlbWEiOiJxdWlwdXgiLCJpZHMiOiI4MTksODIwIiwiaXhwIjoxNTA0MTA5ODI1fQ.30GWfVSUwzGX_GWYs_Gv16BwPKmIkyuu5Xw8zL92Vcc
```

Encoded <small>PASTE A TOKEN HERE</small>	Decoded <small>EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)</small>						
<pre>eyJhbGciOiJIUzI1NiJ9.eyJzZWR1bGEiOiIxMjM0NTY3ODIsInNpc3RlbWEiOiJxdWlwdXgiLCJpZHMiOiI4MTksODIwIiwiaXhwIjoxNTA0MTA5ODI1fQ.30GWfVSUwzGX_GWYs_Gv16BwPKmIkyuu5Xw8zL92Vcc</pre>	<table border="1"><tr><td>HEADER: ALGORITHM &amp; TOKEN TYPE</td></tr><tr><td><pre>{   "alg": "HS256" }</pre></td></tr><tr><td>PAYLOAD: DATA</td></tr><tr><td><pre>{   "cedula": "12345678",   "sistema": "quipux",   "ids": "819, 820",   "exp": "1504109825" }</pre></td></tr><tr><td>VERIFY SIGNATURE</td></tr><tr><td><pre>HMACSHA256(   base64UrlEncode(header) + "." +   base64UrlEncode(payload),   secret ) <input type="checkbox"/> secret base64 encoded</pre></td></tr></table>	HEADER: ALGORITHM & TOKEN TYPE	<pre>{   "alg": "HS256" }</pre>	PAYLOAD: DATA	<pre>{   "cedula": "12345678",   "sistema": "quipux",   "ids": "819, 820",   "exp": "1504109825" }</pre>	VERIFY SIGNATURE	<pre>HMACSHA256(   base64UrlEncode(header) + "." +   base64UrlEncode(payload),   secret ) <input type="checkbox"/> secret base64 encoded</pre>
HEADER: ALGORITHM & TOKEN TYPE							
<pre>{   "alg": "HS256" }</pre>							
PAYLOAD: DATA							
<pre>{   "cedula": "12345678",   "sistema": "quipux",   "ids": "819, 820",   "exp": "1504109825" }</pre>							
VERIFY SIGNATURE							
<pre>HMACSHA256(   base64UrlEncode(header) + "." +   base64UrlEncode(payload),   secret ) <input type="checkbox"/> secret base64 encoded</pre>							

El primer componente:

```
eyJhbGciOiJIUzI1NiJ9
```

representa el algoritmo de firma digital utilizado para verificar los contenidos del token JWT. Se utiliza el algoritmo *HS256*:

```
{  
  "alg": "HS256"  
}
```



## 14. Pruebas de Servicio Web SOAP

Los siguientes ejercicios, se realizaron enviando 1 documento en formato PDF generado en blanco, utilizando el servicio web [https://impws.firmadigital.gob.ec/soap/ws\\_firma\\_digital.php?wsdl](https://impws.firmadigital.gob.ec/soap/ws_firma_digital.php?wsdl)

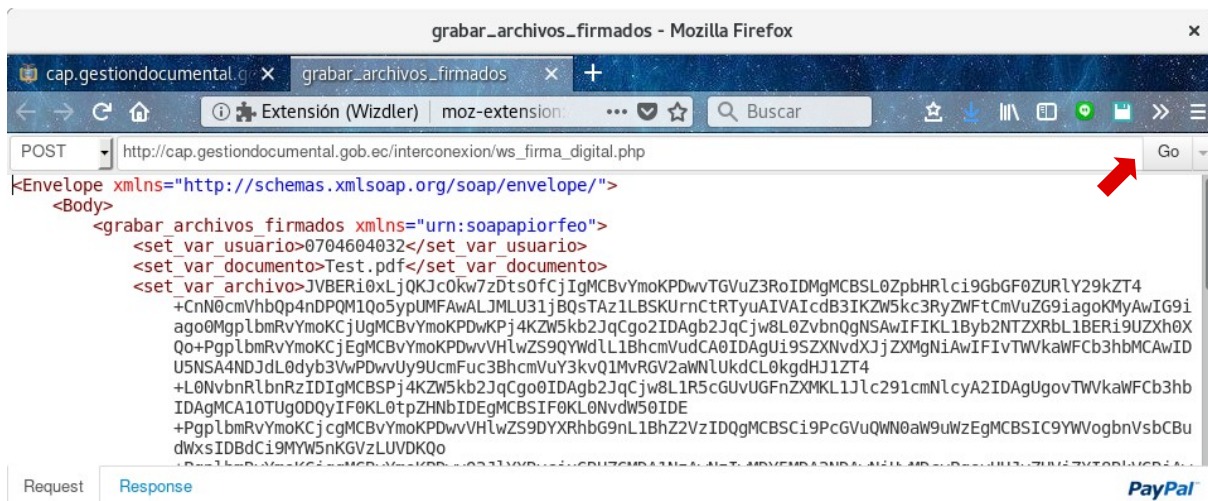
### 14.1 Navegador Firefox (Instalar Extensión Wizdler)

Mayor información en el siguiente link: <https://addons.mozilla.org/en-US/firefox/addon/wizdler/>

Después de instalado, se debe dar clic en el ícono que apunta la flecha y luego seleccionar “grabar\_archivos\_firmados”.



Ingresar la siguiente información (ver archivo adjunto “soap”) y clic en “Go”.





## 15. Glosario de términos

MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información.
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones.
FIRMA ELECTRÓNICA	Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.
CERTIFICADO DE FIRMA ELECTRÓNICA	Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.
ENTIDAD CERTIFICADORA	<b>Entidades de certificación de información.-</b> Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el ARCOTEL.
TOKEN	Dispositivo electrónico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.
DRIVER	Software que permite al equipo reconocer el token.

### Firmas de responsabilidad

Elaborado Por:

Revisado y aprobado Por:

---

Ing. Misael Vladimir Fernández Correa  
**Especialista de Desarrollo de  
Servicios de Gobierno Electrónico**

---

Ing. Pablo Javier Veintimilla Vargas  
**Director de Provisión de Servicios  
Electrónicos**