MANUAL DE USO DEL CERTIFICADO POR SOFTWARE

"USUARIO"

Unidad de Innovación y Desarrollo

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	Alberto Daniel Inch Sáinz		Alberto Daniel Inch Sáinz
Cargo:	Jefe de la Unidad de Innovación y Desarrollo		Jefe de la Unidad de Innovación y Desarrollo
Firma:			
Fecha:	27/06/2019		27/06/2019

MANUAL DE CERTIFICADO POR SOFTWARE - Usuario

1. Certificado por Software....3
2. Conceptos básicos....3
2.1. Par de claves....3
2.2. Certificado de firma digital....3
2.3. Entidad Certificadora Autorizada....4
2.4. Dispositivo criptográfico por software....4
3. Preparando el dispositivo criptográfico por software listo para firmar....4
3.1. Generar par de claves....5
3.2. Guardar dispositivo criptográfico por software....6
3.3. Abrir dispositivo criptográfico por software....7
3.4. Generación de CSR....8
3.5. Cargado del certificado....9
4. Firma de documentos PDF....10

1. Certificado por Software

La firma digital en Bolivia nace como una alternativa a la firma manuscrita en el mundo de los documentos digitales el año 2016, para lo cual era necesario hacer uso de dispositivos criptográficos específicamente diseñados para la generación de par de claves. Sin embargo dada la necesidad de utilizar firma digital en sistemas de forma automática, el año 2019 se amplía la posibilidad de utilizar firma digital por software, es decir delegando a un programa la generación de par de claves.

Al eliminar la dependencia de dispositivos criptográficos, surge la necesidad de contar con un programa que se encargue de la generación del par de claves, al cual se lo denominó "Certificado por Software" y que puede ser descargado de la siguiente URL: https://firmadigital.bo/software. Así mismo es de código abierto por lo que el código fuente está disponible en: https://gitlab.softwarelibre.gob.bo/adsib/certificado-software.

2. Conceptos básicos

En términos simples la firma digital es el equivalente a la firma manuscrita en el mundo de los documentos digitales. Sin embargo para poder hacer uso de esta se debe comprender los siguientes conceptos:

2.1. Par de claves

La firma digital se basa en criptografía asimétrica, la cual se compone de un par de claves: "Clave privada" que sirve para firmar y "Clave pública" que sirve para validar la firma.

2.2. Certificado de firma digital

El certificado de firma digital viene a ser la "Clave pública" del signatario además de sus datos de identidad, ci, nombre entre otros.

2.3. Entidad Certificadora Autorizada

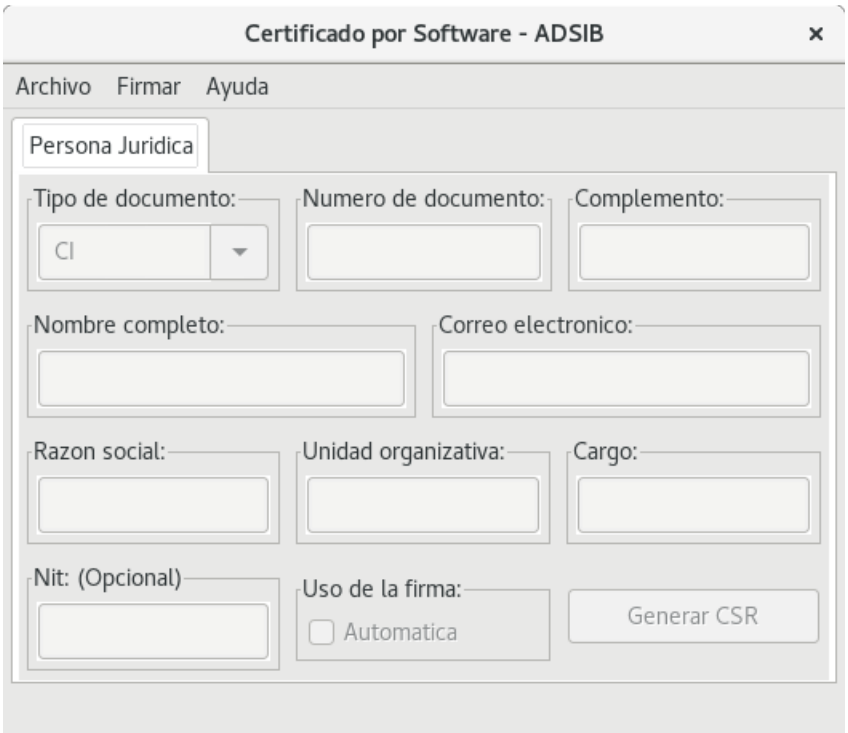
La Entidad Certificadora Autorizada ECA es la encargada de emitir Certificados de firma digital. Para que una firma digital tenga valor legal, debe contar con un Certificado de firma ditial emitido por una ECA autorizada por la ATT.

2.4. Dispositivo criptográfico por software

El dispositivo criptográfico por software es un archivo con extensión p12 o pfx que contiene la clave privada del signatario y el certificado de firma digital cifrados por un algoritmo de criptografía simétrica que protege el contenido por contraseña.

3. Preparando el dispositivo criptográfico por software listo para firmar

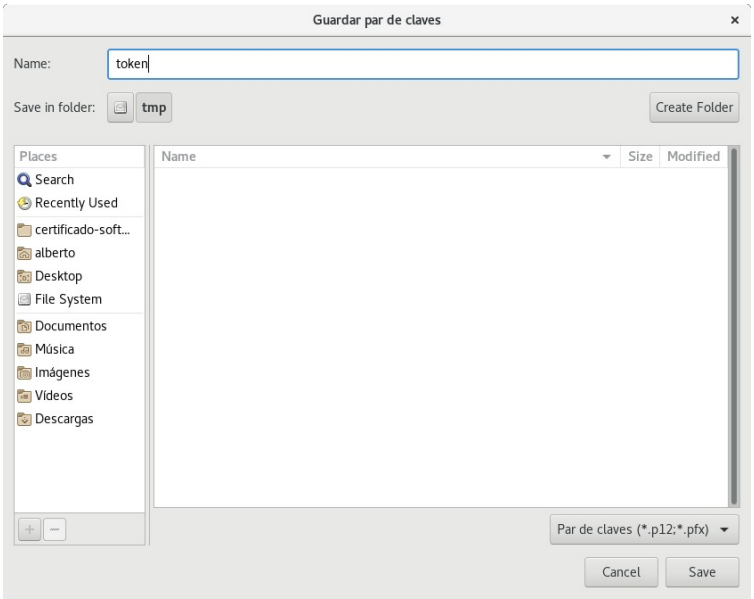
Para contar con un dispositivo criptográfico listo para firmar documentos digitales, se debe iniciar el aplicativo “Certificado por Software” que desplegará la siguiente interfaz:



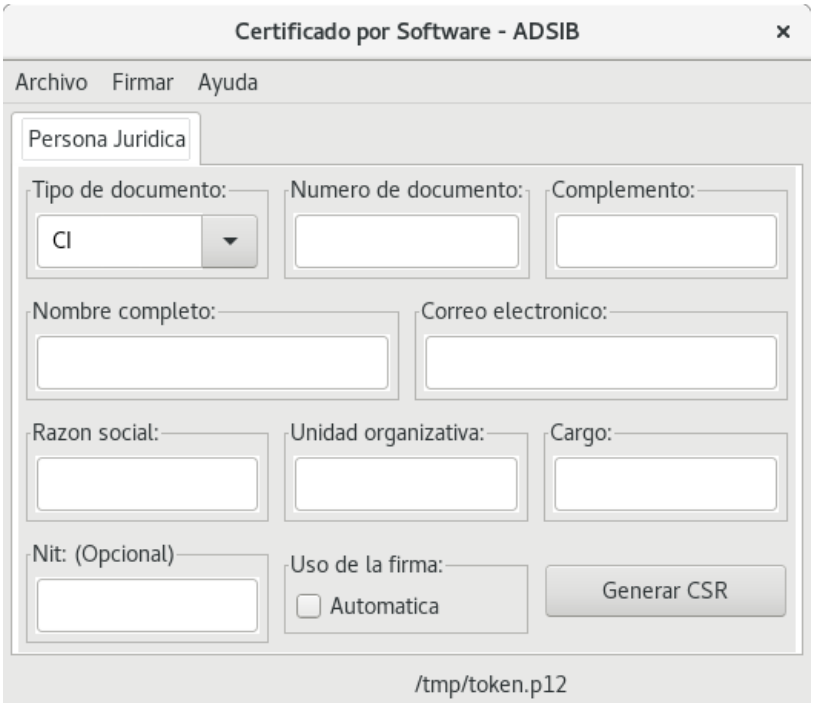
Para crear un nuevo dispositivo p12, una vez dentro, se debe seguir los siguientes pasos:

3.1. Generar par de claves

La generación de par de claves se la realiza a través del menú Archivo->Nuevo que nos desplegará la siguiente interfaz:



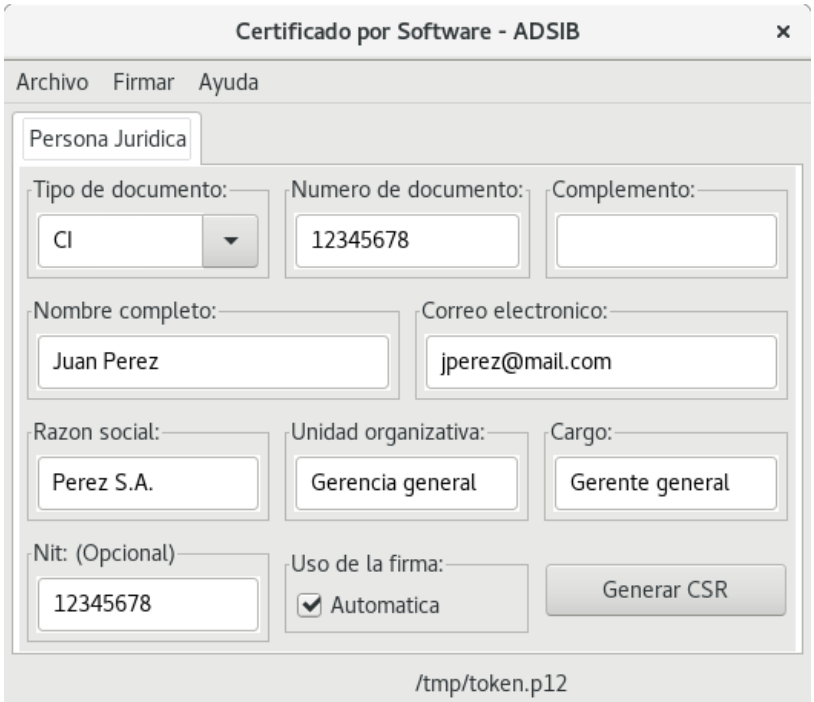
En la cual se debe introducir un nombre para el archivo p12 en la ruta que se desea sea creado este archivo.



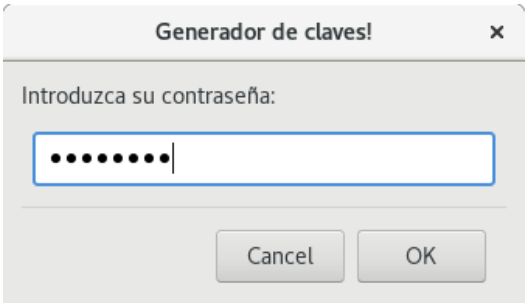
Con esto se crea el par de claves y se tiene todo listo para comenzar a trabajar. Los campos para llenar la identidad del signatario se habilitan para que puedan ser llenados.

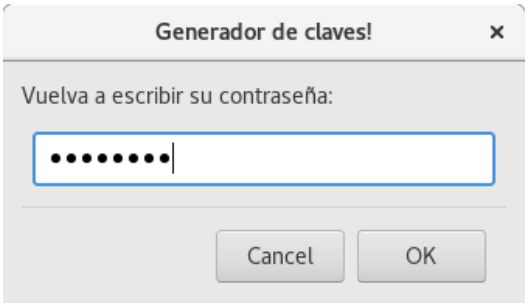
El archivo p12 no será creado hasta que se seleccione el menú Archivo->Guardar o hasta que se genere un CSR.

3.2. Guardar dispositivo criptográfico por software



Para guardar el par de claves y los datos de identidad introducidos, se debe seleccionar el menú Archivo->Guardar para lo que se solicitará una contraseña y la confirmación para verificar que esté bien escrita.

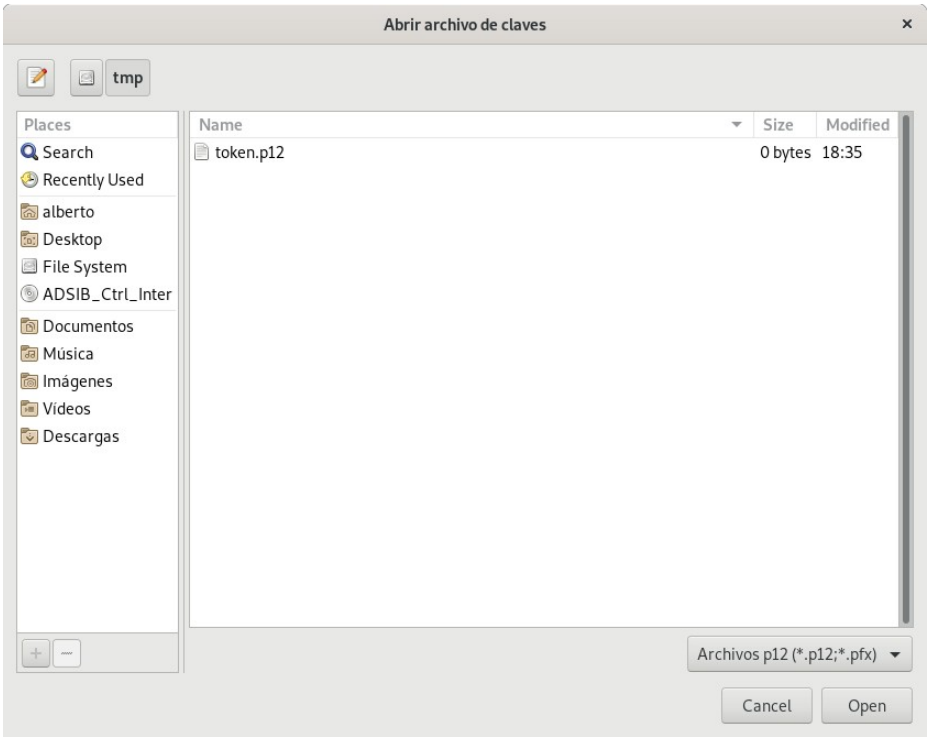




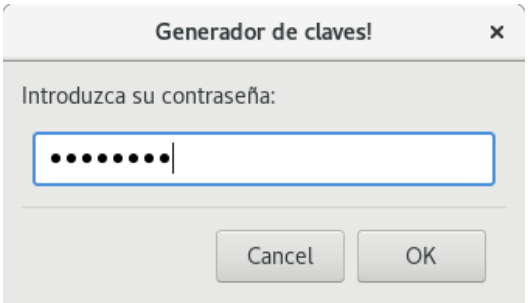
Durante el proceso de emisión de certificado para firma digital, se le preguntará varias veces la contraseña. En todo el proceso siempre se hará referencia a la misma contraseña y la contraseña siempre se utilizara para almacenar la clave privada y el certificado en el archivo p12.

3.3. Abrir dispositivo criptográfico por software

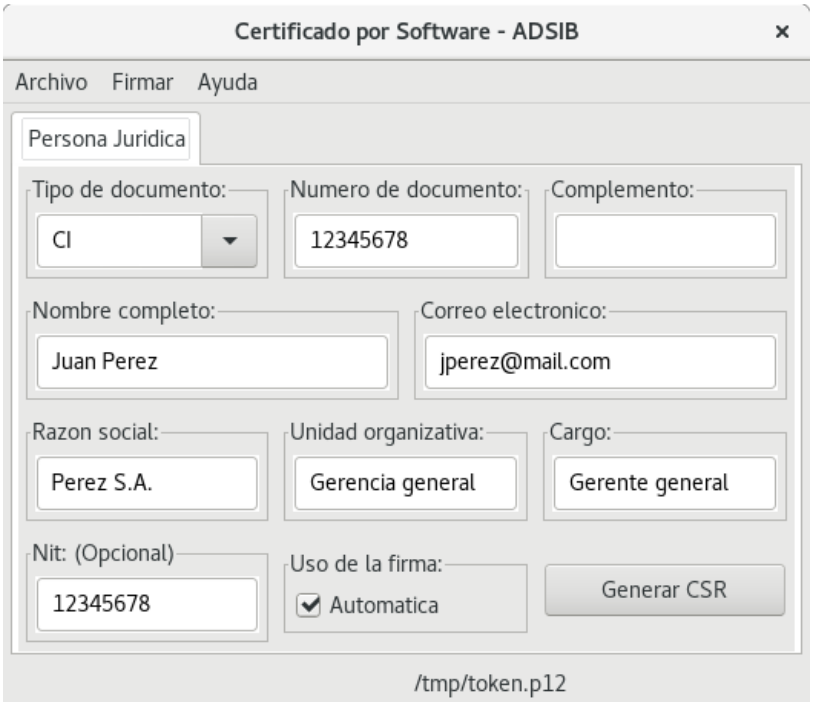
Una vez se ha guardado la clave privada en el dispositivo criptográfico p12, se podrá recuperar en cualquier momento a través del menú Archivo->Abrir que desplegará la siguiente interfaz:



A continuación, una vez seleccionado el archivo p12 se solicitará la contraseña con la cual se almacenó la clave privada:



Y una vez introducida, se abrirá mostrando los datos de identidad introducidos antes de guardar el archivo p12.



3.4. Generación de CSR

Con los pasos anteriores se puede observar que ya se tiene disponible un dispositivo p12 con un certificado autofirmado y la clave privada por lo que ya se podría firmar documentos haciendo uso del archivo generado. Sin embargo un certificado autofirmado al no estar avalado por una Entidad Certificadora Autorizada no tendrá ningún valor legal.

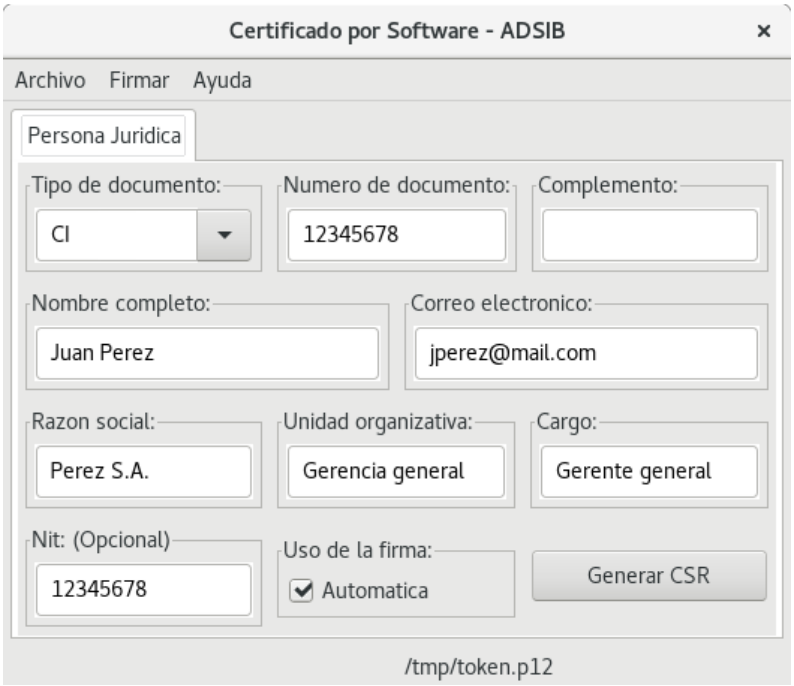
En el subtítulo 2.3 se explicaba que para que una firma digital tenga valor legar, deberá contar con un certificado emitido por una Entidad Certificadora Autorizada. Para que la ECA emita un certificado compatible con la Clave Privada del archivo p12 es necesario un paso intermedio conocido como Solicitud de Firma de Certificado CSR por sus siglas en inglés.

El CSR no es más que un archivo que contiene la clave pública con los datos de identidad y que se envía a la ECA para que emita el certificado en base a la información contenida.

Para generar este archivo, bastará con hacer clic sobre el botón Generar CSR. En caso de que se haya modificado los datos de identidad o que no se haya guardado aún el archivo p12, se preguntará por la contraseña para almacenar los datos actualizados tal cual se exportan al CSR. Se guardará el archivo p12 actualizado y se preguntará por el nombre y ruta para el archivo CSR que finalmente será exportado.

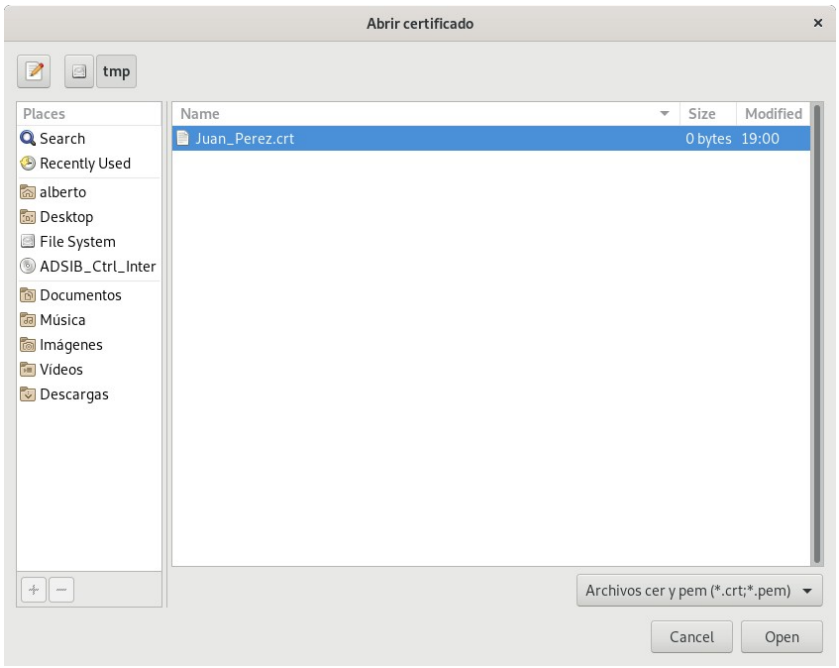
3.5. Cargado del certificado

Una vez se tiene disponible el certificado emitido por la ECA, el mismo deberá ser guardado juntamente con la clave privada en el archivo p12. Para lo cual se debe tener abierto el archivo p12.



En caso de que se lo haya cerrado se lo puede abrir con el menú Archivo->Abrir. De ninguna manera se debe crear un nuevo par de claves con el certificado ya emitido debido a que una nueva clave privada no se podrá emparejar con el certificado.

Para cargar el certificado, simplemente seleccionar el menú Archivo->Cargar Certificado, lo cual desplegará la siguiente interfaz.



Una vez cargado se muestra un mensaje de confirmación con lo que el dispositivo criptográfico por software se encuentra listo para firmar.

4. Firma de documentos PDF

Con el dispositivo criptográfico por software listo como se indica en la anterior sección, es posible firmar documentos PDF desde esta misma aplicación a través del menú Firmar->Firmar PDF.