



IPSSSET
INSTITUTO DE PREVISIÓN Y SEGURIDAD
SOCIAL DEL ESTADO DE TAMAULIPAS



100 años: Educación para todos

Artículo 3º
Constitucional LAICA
GRATUITA
OBLIGATORIA

"EN TAMAULIPAS DEFENDEMOS LA ESCUELA PÚBLICA"

Generador de Requerimiento de Certificado de Firma Electrónica Avanzada ®

Contenido

Prefacio.....	3
Dirigido a	3
Estructura del Documento	3
Capítulo 1: Requisitos Previos.....	3
Capítulo 2: Marco Legal.....	3
Capítulo 3: Introducción	3
Capítulo 4: Instalación	3
Capítulo 5: Forma de operar	4
Capítulo 6: Desinstalación	4
Requisitos Previos	5
Requisitos de Hardware.....	5
Requisitos de Software	5
Introducción.....	6
Firma.....	6
Firma Electrónica	6
Firma Electrónica Avanzada	6
Funcionamiento de la firma electrónica.....	6
Generador de requerimiento de certificado de Firma Electrónica Acreditada. ...	7
Procedimiento de descarga de la aplicación	7
Instalar Aplicación.....	9
Acceso desde el menú de programas	12
1. Generación de solicitud de certificado digital.....	13
2. Verificación y validación de archivo de firma electrónica avanzada	17
3.. Información.....	21
Desinstalación	22

Prefacio

Este manual describe la forma de operar a nivel de usuario el “Generador de Requerimiento de Certificado de Firma Electrónica Avanzada” en una computadora de escritorio o portátil con sistema operativo Windows en su versión 2000/XP o superior. Los puntos a cubrir en éste prefacio son:

- Dirigido a
- Estructura del documento

Dirigido a

Las instrucciones para la configuración y administración del están dirigidas:

- Usuarios con las facultades para administrar y configurar sesiones del programa “Generador de Requerimiento de Firma Electrónica UPYSSET/SARTET” en el equipo, con una comprensión del sistema operativo básico.
- Usuarios con la necesidad de generar solicitudes de certificados digitales y archivos de firma electrónica avanzada.

Estructura del Documento

Capítulo 1: Requisitos Previos

Hace referencia a los requerimientos de hardware y software que el equipo de cómputo debe cumplir para usar el “Generador de Requerimiento de Certificado de Firma Electrónica Acreditada”.

Capítulo 2: Marco Legal

Hace referencia a las leyes que dieron origen al “Generador de Requerimiento de Certificado de Firma Electrónica Acreditada”.

Capítulo 3: Introducción

Conceptos relacionados con el “Generador de Requerimiento de Certificado de Firma Electrónica Acreditada”.

Capítulo 4: Instalación

Indica los pasos a seguir para instalar el “Generador de Requerimiento de Certificado de Firma Electrónica Acreditada”.

Capítulo 5: Forma de operar

Establece la forma adecuada de proceder para utilizar el “Generador de Requerimiento de Certificado de Firma Electrónica Acreditada”.

Capítulo 6: Desinstalación

Indica los pasos a seguir para desinstalar el “Generador de Requerimiento de Certificado de Firma Electrónica Acreditada”.

Requisitos Previos

Es muy importante tomar en cuenta las siguientes recomendaciones de hardware y software para que el programa “Generador de Requerimiento de Certificado de Firma Electrónica Acreditada” funcione adecuadamente.

Requisitos de Hardware

- Procesador Intel Pentium IV o equivalente a 2 GHz.
- Memoria RAM de 256 MB o superior.
- Espacio en Disco Duro de 10 MB o superior.

Requisitos de Software

- Sistema Operativo Windows XP, Windows 7, Windows 10.
- Microsoft .net Framework 2.0 o superior.

Introducción

Glosario de términos

Firma

A un pequeño símbolo, palabra o ambos que permite identificar y asegurar la identidad de un autor o remitente se le conoce como firma o firma autógrafa. Está es el lazo que une al firmante con un documento como prueba del consentimiento y/o verificación de la integridad y aprobación de la información contenida en el mismo.

Tradicionalmente se realiza de forma manuscrita, el firmante escribe una palabra y/o una serie de trazos personales que le identifican como tal. En caso de duda un Perito Calígrafo podría determinar si una firma pertenece a una determinada persona o si se trata de una falsificación. De tal modo que una firma autógrafa contiene las siguientes características: es identificativa, declarativa y probatoria.

Firma Electrónica

La firma electrónica es una tecnología que produce los mismos efectos jurídicos que la "firma autógrafa" de un documento físico, siendo también admisible como prueba en juicio, en función de la legislación vigente. Esta tecnología se basa en la criptografía. Mediante mecanismos criptográficos, se lleva a cabo la firma electrónica y su posterior confirmación y validación.

Firma Electrónica Avanzada

En términos prácticos, la firma electrónica avanzada consiste en un conjunto de datos asociados a un mensaje o documento electrónico, que permite garantizar con total seguridad la identidad del firmante y la integridad del texto o mensaje enviado.

Funcionamiento de la firma electrónica.

Se basa en el uso de un par de llaves, que son un par de números matemáticamente relacionados, Al primero se le denomina llave pública y al segundo llave privada. Un programa de cómputo los produce los entrega a un solicitante, quien puede dar a conocer la primera y debe mantener en secreto la segunda.

Cada llave es la función inversa de la otra, es decir, lo que con una llave se asegura con la otra llave se valida.

Generador de requerimiento de certificado de Firma Electrónica Acreditada.

El Generador de Requerimiento de certificado de Firma Electrónica Acreditada, es un sistema que cuenta con dos funciones. En primer lugar, permite crear una solicitud de un certificado digital. Mediante este procedimiento se generan las llaves pública y privada del solicitante. Una vez obtenido el certificado, permite verificar y crear el archivo de firma electrónica acreditada que es necesario para las aplicaciones donde será aplicada.

Instalación

Procedimiento de descarga de la aplicación

Como primer paso deberá acceder al sitio en internet de la Firma Electrónica de IPSSET-SARTET. La página de acceso se encuentra en la dirección:

<https://ca.advantage-security.com/acipsset-sartet/>

Una vez en el sitio, se debe seleccionar la opción “Descargas Herramientas y Manuales”

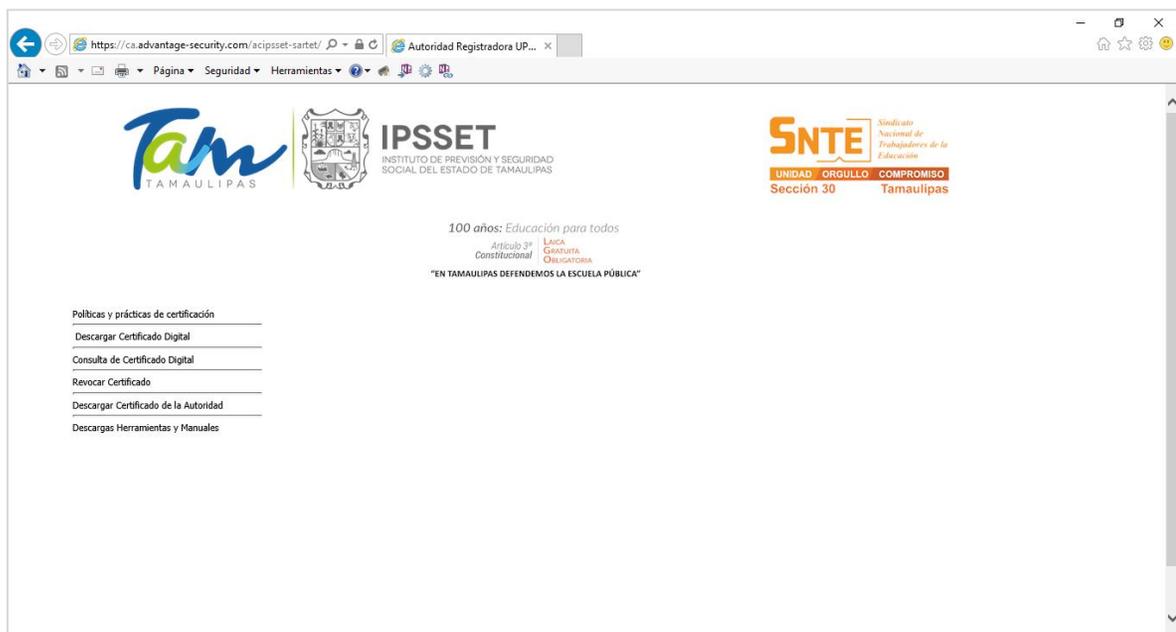


Figura 0-1 Sitio Autoridad Registradora IPSSET-SARTET

La opción “Descargas Herramientas y Manuales”, permite descargar las siguientes opciones:

1. Generador de requerimientos Generador de Requerimientos IPSSET/SARTET 2.3
2. Descargar Guía de usuario, Generador de Requerimientos Generador de Requerimientos IPSSET/SARTET 2.3
3. Descargar Solicitud de Certificado de Firma Electrónica Avanzada

Así mismo cuenta con un vínculo para descargar el “Framework 2.0” de Microsoft, el cual es un prerequisite para el software generador de requerimientos.

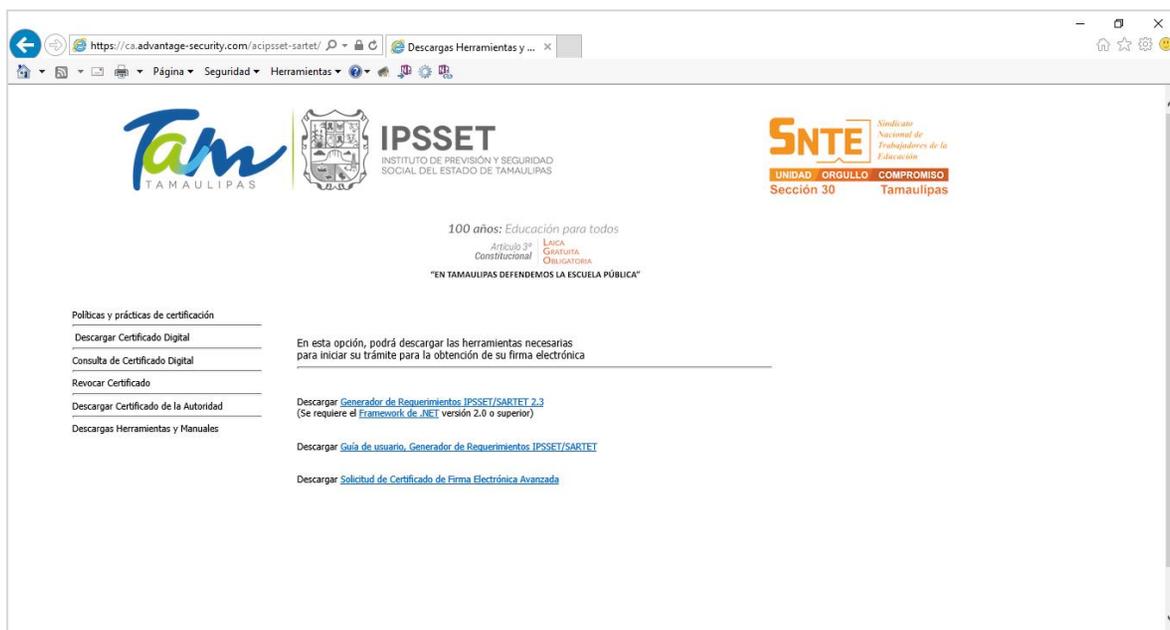


Figura 0-2 Descargas y Manuales

- La opción "Generador de Requerimientos IPSSET/SARTET 2.3", podrá descargar un archivo en formato comprimido que contiene el programa Generador de Solicitudes de Certificados Digitales, el cual es necesario instalar como se enuncia a continuación:
- La opción de “Descargar Guía de Usuario, Generador de Requerimiento”, podrá descargar la presente guía.
- La opción de “Descargar Solicitud de Certificado de Firma Electrónica Avanzada”, podrá descargar los lineamientos bajo los cuales opera la firma electrónica del SARTET.

Instalar Aplicación

En este capítulo se describe el proceso de instalación del “Generador de Requerimiento de certificado de Firma Electrónica Avanzada”

Nota: Es importante que antes de iniciar la instalación cierre todas las aplicaciones para evitar que interfieran con el proceso.

Descomprimir el archivo “*Setup GenRequest.msi*”. Para descomprimir el archivo se podrán utilizar la opción de “Extraer todo...” provista por el sistema operativo o bien utilizar algún programa que maneje archivos comprimidos. Se debe extraer el archivo *Setup GenRequest.msi*

Ejecutar el instalador “*Setup GenRequest.msi*”. Aparecerá la siguiente pantalla.

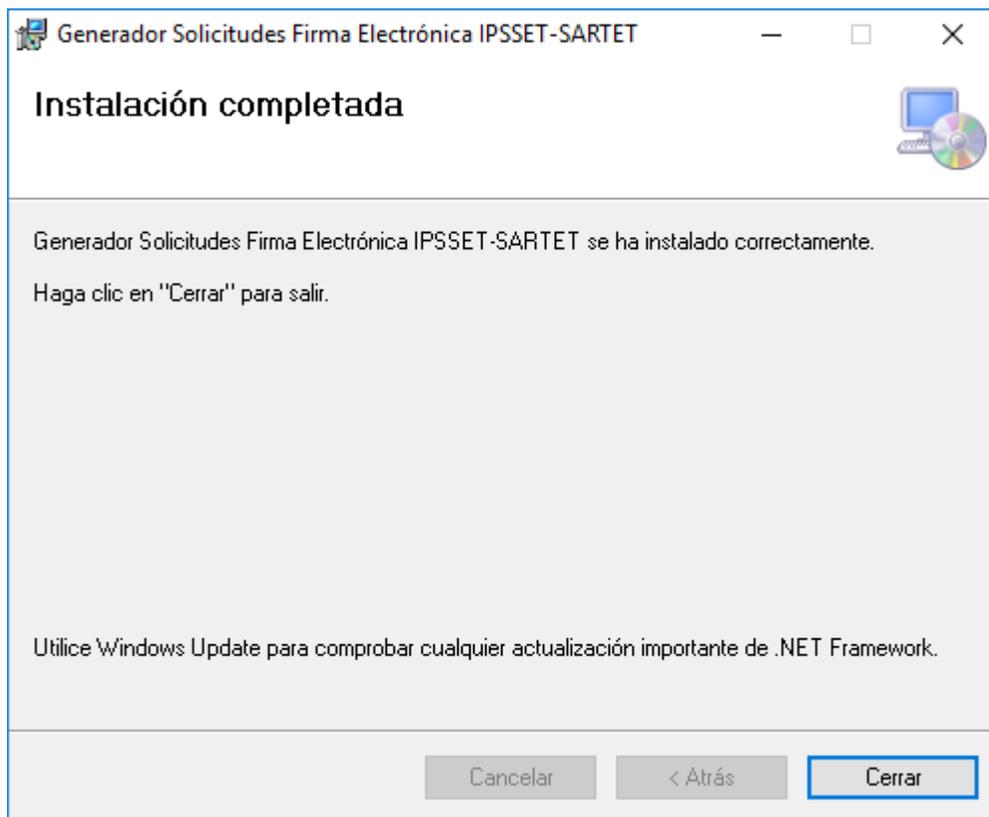


Figura 0-3 Asistente para la instalación

Dar clic en el botón “Siguiente>”, y el asistente de instalación mostrará una pantalla donde se describe la ruta de instalación de la aplicación.

En caso de requerirse, dar clic en examinar para seleccionar otra carpeta.

Seleccionar si la aplicación va a ser utilizada por todos los usuarios de este equipo o sólo para el que la está instalando (se recomienda permitir la ejecución a todos los usuarios).

Dar clic en el botón “Siguiente>”.

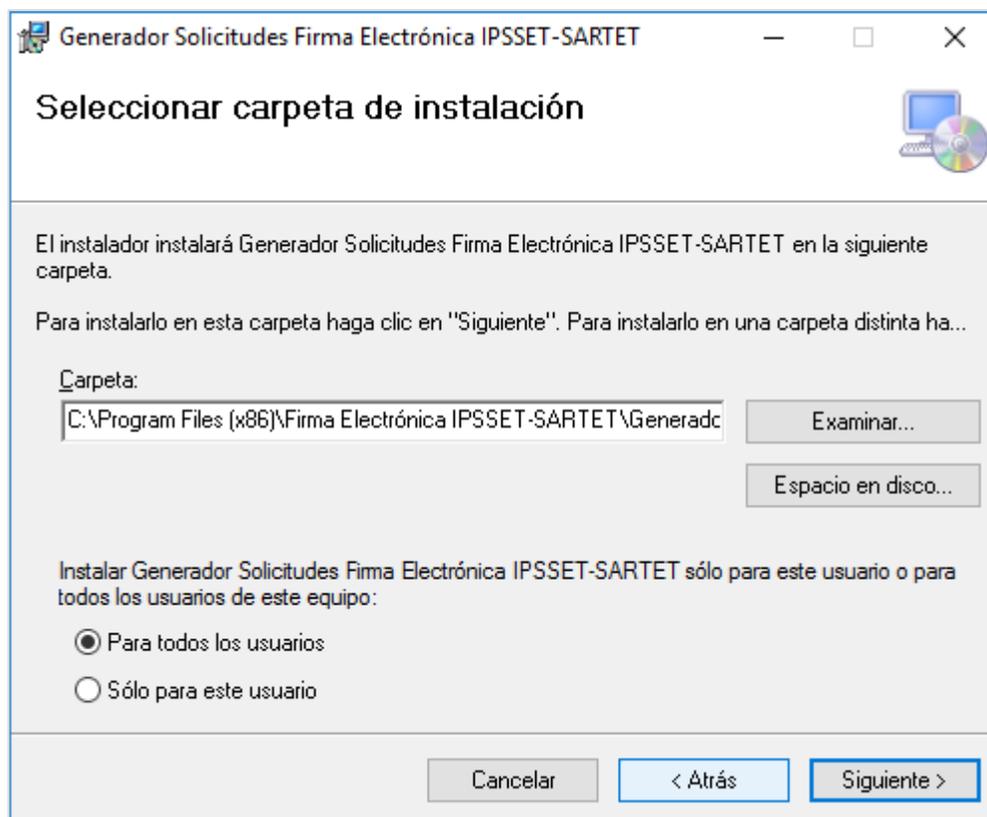


Figura 0-4 Seleccionar carpeta para la instalación.

Finalmente, el instalador solicitará confirmar la instalación para lo cual se debe seleccionar el botón “Siguiente>”

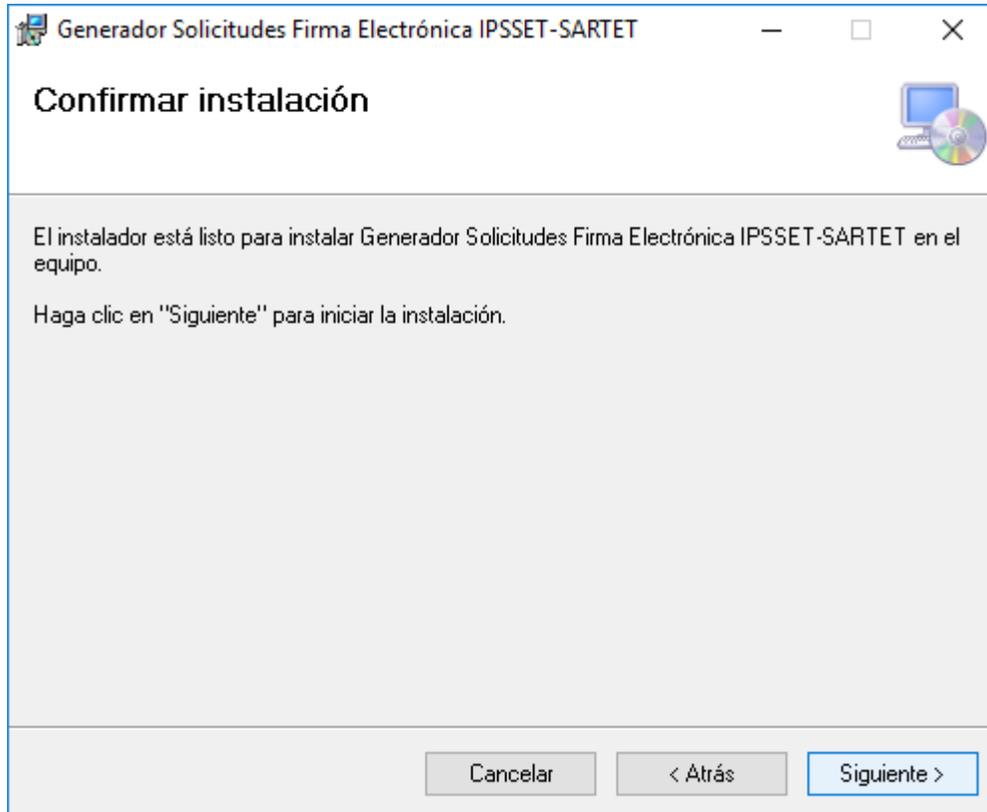


Figura 0-5 Confirmar instalación

El asistente de instalación desplegará el progreso de la instalación tal como se ilustra en la siguiente figura.

Una vez finalizado el proceso de instalación, el asistente desplegará una pantalla indicando que la instalación se ha completado. Se deberá seleccionar el botón “Cerrar”

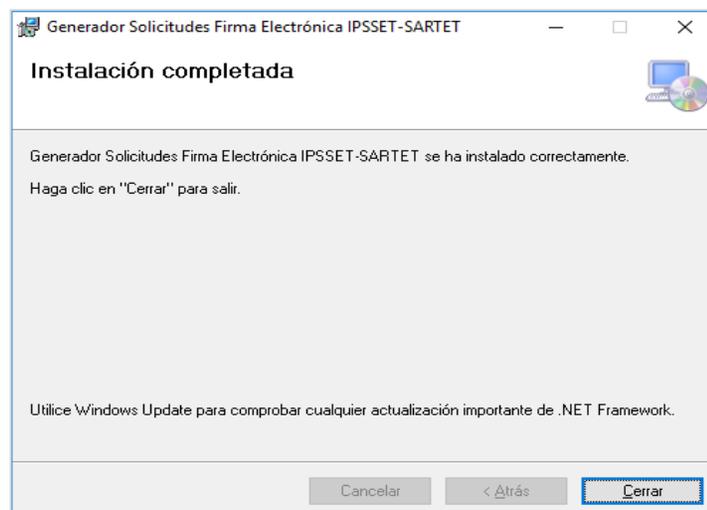


Figura 0-6 Finalizar Instalación

Forma de operar

Una vez que se ha instalado el programa “Generador Solicitudes de Firma Electrónica IPSSET-SARTET” se podrá acceder desde un acceso directo instalado en el escritorio del equipo o desde el grupo de programas “Generador Solicitud de Firma Electrónica IPSSET-SARTET” del menú de programas instalados en el equipo.



Acceso desde el menú de programas

El procedimiento se detalla a continuación.

1. Dar clic en el botón de Inicio
2. Dar clic sobre la opción Programas
3. Dar clic sobre la opción de Generador Firma Electrónica IPSSET-SARTET
4. Dar clic sobre la opción Solicitud de Certificado
5. Dar clic sobre la opción Firma Electrónica IPSSET-SARTET

Una vez seleccionada la opción se muestra la siguiente pantalla:

La interfaz de usuario muestra el título 'Firma Electrónica IPSSET-SARTET' y el logo de TAMAULIPAS. A la derecha se encuentran los logos de IPSSET (INSTITUTO DE PREVISIÓN Y SEGURIDAD SOCIAL DEL ESTADO DE TAMAULIPAS) y SNTE (Sindicato Nacional de Trabajadores de la Educación). En el centro, se menciona '100 años: Educación para todos' y 'Artículo 3º Constitucional LAICA GRATUITA OBLIGATORIA'. Debajo de esto, se lee 'EN TAMAULIPAS DEFENDEMOS LA ESCUELA PÚBLICA'. A la derecha del SNTE se indica 'UNIDAD ORGULLO COMPROMISO Sección 30 Tamaulipas'.

Generación de Solicitud Certificado Digital	En esta aplicación encontrará las siguientes opciones
Verificación y Creación de Archivo Firma Electrónica Avanzada	Generación de solicitud de certificado digital. Esta opción le permitirá capturar sus datos personales los cuales serán relacionados de manera única a la solicitud de certificado digital.
Renovación de Solicitud Certificado Digital	Verificación y creación de archivo de firma electrónica avanzada. Esta opción completa el proceso de generación de su archivo para la aplicación de firma electrónica.
Información	Renovación de solicitud de certificado digital. Esta opción le permitirá renovar su certificado digital. Debe poseer una conexión a Internet para realizar la actualización

Versión 2.3
2016 Derechos Reservados



Figura 0-7 Inicio del Generador de Solicitudes

Esta pantalla es el menú principal de la aplicación y permite el acceso a 3 funciones:

1. Generación de solicitud de certificado digital.
2. Verificación y creación de archivo de firma electrónica avanzada.
3. Información.

1. Generación de solicitud de certificado digital

Esta opción permite la generación de una solicitud de certificado digital, lo cual implica la generación del par de llaves (pública y privada), además de proporcionar los datos de identificación. Este proceso consta de 4 etapas:

Paso 1/4: Acuerdo del solicitante.

Establece los términos y condiciones:

Firma Electrónica IPSSET-SARTET

100 años: Educación para todos
 Artículo 3º Constitucional LAICA GRATUITA OBLIGATORIA
 "EN TAMAULIPAS DEFENDEMOS LA ESCUELA PÚBLICA"

Generación de Solicitud Certificado Digital	Generación de Solicitud de Certificado Digital (paso 1/4) Acuerdo del solicitante
Verificación y Creación de Archivo Firma Electrónica Avanzada	Al iniciar con su proceso de solicitud de certificado digital se asume que está de acuerdo con los términos y condiciones descritos en el Acuerdo de Suscriptor
Renovación de Solicitud Certificado Digital	<p>TÉRMINOS Y CONDICIONES DE USO:</p> <p>El suscrito (usuario), cuyos datos generales aparecen integrados a la presente solicitud, manifiesto que es mi libre voluntad contar con un certificado de Firma Electrónica Avanzada en el que conste la clave pública que se encuentra asociada a la clave privada y su correspondiente frase de seguridad, misma que manifiesto haber generado previamente y en absoluto secreto, sin que persona alguna me haya asistido durante dicho proceso.</p> <p>El solicitante en este acto acepta el certificado digital mencionado, sirviendo el presente documento como el acuse de recibo en el más amplio sentido que en derecho proceda.</p> <p>Adicionalmente, el solicitante, acepta que el uso de su clave privada y su frase de seguridad, con base en los cuales su certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma</p>
Información	

Cancel Aceptar

Versión 2.3
2016 Derechos Reservados

Figura 0-8 Acuerdo del solicitante

Dar clic en aceptar.

Firma Electrónica IPSSET-SARTET

100 años: Educación para todos
 Artículo 3º Constitucional LAICA GRATUITA OBLIGATORIA
 "EN TAMAULIPAS DEFENDEMOS LA ESCUELA PÚBLICA"

Generación de Solicitud Certificado Digital	Generación de Solicitud de Certificado Digital (paso 2/4) Datos del solicitante Nombre(s), Apellidos: <input type="text"/> RFC: <input type="text"/> CURP: <input type="text"/> Correo electrónico: <input type="text"/> Sección Sindical: <input type="text" value="30"/> Municipio Laboral: <input type="text"/> Municipio Particular: <input type="text"/> Estado: <input type="text" value="TAMAULIPAS"/> País: <input type="text" value="MX"/> Frase de revocación Frase: <input type="text"/> Confirmación: <input type="text"/> <input type="button" value="Cancelar"/> <input type="button" value="Aceptar"/>
Verificación y Creación de Archivo Firma Electrónica Avanzada	
Renovación de Solicitud Certificado Digital	
Información	

Versión 2.3
2016 Derechos Reservados

Figura 0-9 Datos del solicitante y frase de revocación
Paso 2/4: Ingreso de los datos del solicitante y la frase de revocación.

Todos los campos son obligatorios a excepción del correo electrónico y de describen a continuación:

Tabla 1.1 Información del solicitante y la frase de revocación

Campo	Descripción
Nombre(s) Apellidos	Nombre completo del solicitante empezando por su primer nombre, seguido de sus apellidos paterno y materno.
RFC	Registro Federal de Contribuyentes del solicitante. Consta de 13 caracteres. En caso de contener menos caracteres el sistema desplegará un error.
CURP	Clave Única de Registro de Población del solicitante. Consta de 18 caracteres. En caso de contener menos caracteres el sistema desplegará un error.
Correo electrónico	Dirección de Correo Electrónico del solicitante.

Sección Sindical	Corresponde a la Sección Sindical a la cual está asignado el solicitante.
Municipio Laboral	Corresponde al Municipio donde labora el solicitante.
Municipio Particular	Corresponde al Municipio donde vive el solicitando
Estado	Es un valor predeterminado. Está asignado a “Tamaulipas”
País	Es un valor predeterminado. Está asignado a “MX”, lo cual representa a México
Frase	Es un conjunto de caracteres que serán usados para validar la revocación del certificado en caso de que la llave privada asociada sea perdida o comprometida.
Confirmación	Es la repetición del campo anterior a fin de asegurarse que se haya escrito correctamente.

Llenar los campos y dar clic en continuar.

Paso 3/4: Asignación de frase de seguridad para la llave privada.

Esta frase es muy importante ya que mediante la misma se protegerá el acceso y uso de la llave privada.

Al proporcionar la clave y dar clic en el botón “Generar”, se solicitará al usuario que seleccione la carpeta en donde se guardarán dos archivos:

1. La clave privada del solicitante. Se generará un archivo con el prefijo “SOLICITUD_” más el dato correspondiente al CURP ingresado y con extensión “.key”.
2. El requerimiento del solicitante. Se generará un archivo con el prefijo “SOLICITUD_” más el dato correspondiente al CURP ingresado y con extensión “.req”. Este archivo es necesario presentar ante la Autoridad Certificadora, para que una vez que haya revisado la documentación correspondiente y acreditada la identidad del solicitante, se genere el certificado.



Figura 0-10 Selección de carpeta para el almacenamiento de la llave privada y el requerimiento del certificado

Seleccionar la carpeta y dar clic en el botón “OK”, el sistema escribirá los dos archivos en la carpeta seleccionada.

Proporciona al solicitante las instrucciones referentes al uso que le debe hacer a los archivos generados.

Al dar clic en aceptar se regresa al menú principal de la aplicación.

Nota: Cuando el solicitante acuda a realizar su trámite de acreditación, no debe llevar consigo el archivo de la llave privada identificado con la extensión “.key”.

2. Verificación y validación de archivo de firma electrónica avanzada

Una vez que el proceso de emisión de Certificado Digital ha sido completado por la Autoridad Certificadora del IPSET-SARTET, se indicará al solicitante como copiar el archivo del certificado digital ya sea desde el portal en internet de la Autoridad Certificadora del IPSET-SARTET, o bien al momento de realizar su trámite le será entregado el archivo con el certificado digital expedido.

El solicitante ingresará nuevamente a la aplicación “Generador Firma Electrónica IPSSSET-SARTET”. Seleccionará la opción “Verificación y Creación de Firma Electrónica Avanzada” para finalmente obtener un tercer archivo el cual contiene los elementos necesarios para poder generar una firma de documentos electrónicamente. Los elementos que reúne son:

1. El certificado del solicitante (que contiene su llave pública).
2. La llave privada del solicitante.

Este proceso consta de dos pasos

Paso 1/2: Generación del “archivo de firma electrónica avanzada”.

En esta sección se proporcionan todos los elementos necesarios para la generación de un archivo de firma electrónica avanzada bajo una estructura de archivo PKCS12. Para generar el archivo de firma electrónica avanzada se requiere del certificado y la llave privada asociada. Este proceso podrá realizarse una vez obtenido el certificado digital emitido por la Autoridad Certificadora.



Figura 0-11 Generación del certificado de firma electrónica avanzada

Así también, en esta opción se describe el certificado digital de la “Autoridad Certificadora de IPSSET-SARTET”.

Seleccionar los archivos solicitados presionando los íconos de Certificado y Llave privada respectivamente. Una vez seleccionados los archivos presionar el botón “Validar”.

Paso 2/2: Verificación del “archivo de firma electrónica avanzada”.

En la primera sección de este paso, se verifica el certificado digital y se muestra la siguiente información asociado al certificado:

1. Nombre
2. Serie del certificado digital
3. Fecha de vencimiento

En la segunda sección de este paso, se solicita la frase de seguridad con que fue protegida la llave privada para acceder a la llave privada. Esta frase es la que se definió en el paso 3 de la opción “Generación de la solicitud de certificado digital”.



Figura 0-12 Verificación del archivo de firma electrónica avanzada

Una vez incorporada la frase de seguridad, y presionado el botón de copiar, se solicitará la carpeta en donde se almacenará el archivo de firma electrónica en formato PKCS12 y cuyo nombre corresponderá al nombre del titular del certificado digital.



Figura 0-13 Almacenamiento del archivo de firma electrónica avanzada

Si la llave privada, el certificado digital y la frase de seguridad son correctos aparecerá el siguiente mensaje.



Figura 0-14 Mensaje de estatus

Firma Electrónica IPSSET-SARTET
✕



TAMAUPLIPAS



IPSSET
INSTITUTO DE PREVISIÓN Y SEGURIDAD
SOCIAL DEL ESTADO DE TAMAUPLIPAS



SNTE
Sindicato Nacional de Trabajadores de la Educación
UNIDAD ORGULLO COMPROMISO
Sección 30 Tamaulipas

100 años: Educación para todos
Artículo 3º Leyes Constitucionales
"EN TAMAUPLIPAS DEFENDEMOS LA ESCUELA PÚBLICA"

Generación de Solicitud Certificado Digital	<p>Verificación y creación de archivo de firma electrónica avanzada (PKCS12) (2 / 2)</p> <p>El certificado digital fue validado correctamente y cuenta con la siguiente información.</p> <p>Nombre: certificado de prueba vpm Serie del certificado digital: 30.30.39.39.39.39.30.30.30.30.31.31.30.30.30.37.32.36.39 Fecha de vencimiento: 2019-03-02 13:24:38</p>
Verificación y Creación de Archivo Firma Electrónica Avanzada	<p>A continuación deberá ingresar la frase de seguridad con que protegió su llave privada y la aplicación generará el archivo con los elementos para generación y aplicación de firma electrónica avanzada.</p>
Renovación de Solicitud Certificado Digital	<p>Frase de seguridad: <input style="width: 150px;" type="password" value="*****"/></p>
Información	<p>Una vez ingresada su frase debe seleccionar el botón "Copiar" y la aplicación solicitará elija una carpeta donde se escribirá el siguiente archivo.</p> <p>certificado de prueba vpm.p12</p> <p>Considere que una vez generado el archivo deberá resguardarlo en un lugar seguro y sólo accesible por usted.</p> <div style="text-align: right; margin-top: 10px;"> Copiar </div>

Versión 1.3
2016 Derechos Reservados

3.. Información

En este apartado, se muestra la versión del producto así como la información de las librerías usadas para la implementación de la herramienta.

Firma Electrónica IPSSET-SARTET

Tam TAMAULIPAS

IPSSET INSTITUTO DE PREVISIÓN Y SEGURIDAD SOCIAL DEL ESTADO DE TAMAULIPAS

SNTE Sindicato Nacional de Trabajadores de la Educación
UNIDAD ORGULLO COMPROMISO
Sección 30 Tamaulipas

100 años: Educación para todos
Artículo 3º Constitucional LAICA GRATUITA OBLIGATORIA
"EN TAMAULIPAS DEFENDEMOS LA ESCUELA PÚBLICA"

Generación de Solicitud Certificado Digital

Verificación y Creación de Archivo Firma Electrónica Avanzada

Renovación de Solicitud Certificado Digital

información

Generador de Solicitudes para Certificado Digital
Versión 2.3

NOTAS:

- * Esta aplicación incluye software desarrollado en el Proyecto OpenSSL, para usarse en el "OpenSSL Toolkit" (<http://www.openssl.org/>)
- * Esta aplicación incluye software de criptografía escrita por Eric Young (eay@cryptosoft.com)
- * Esta aplicación incluye software escrito por Tim Hudson (tjh@cryptosoft.com)

Versión 2.3
2016 Derechos Reservados

Figura 0-15 Versión del sistema y de librerías

Desinstalación

Para desinstalar el producto, es necesario acceder al Panel de Control de Windows. (Inicio -> Configuración -> Panel de Control)

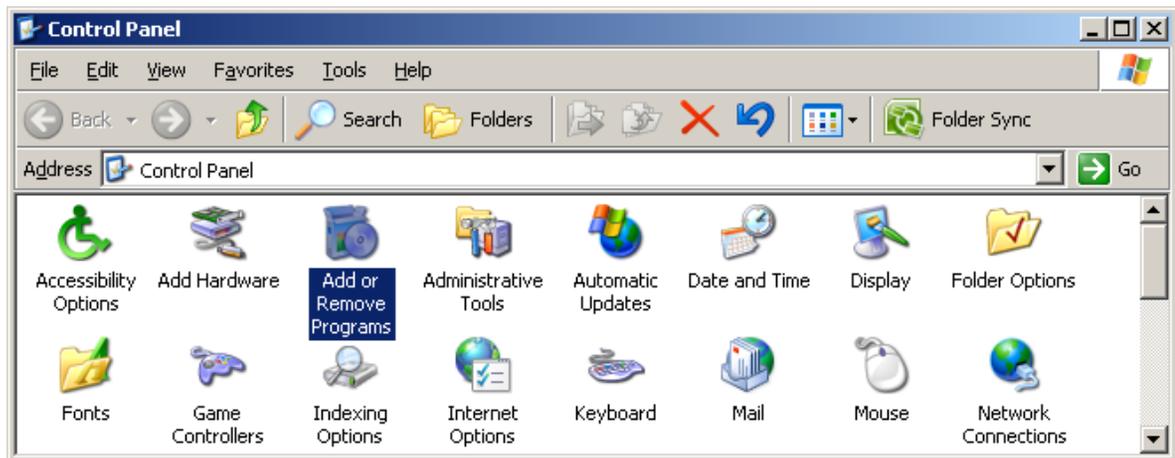


Figura 0-1 - Panel de Control

Y ejecutar “agregar o quitar programas”

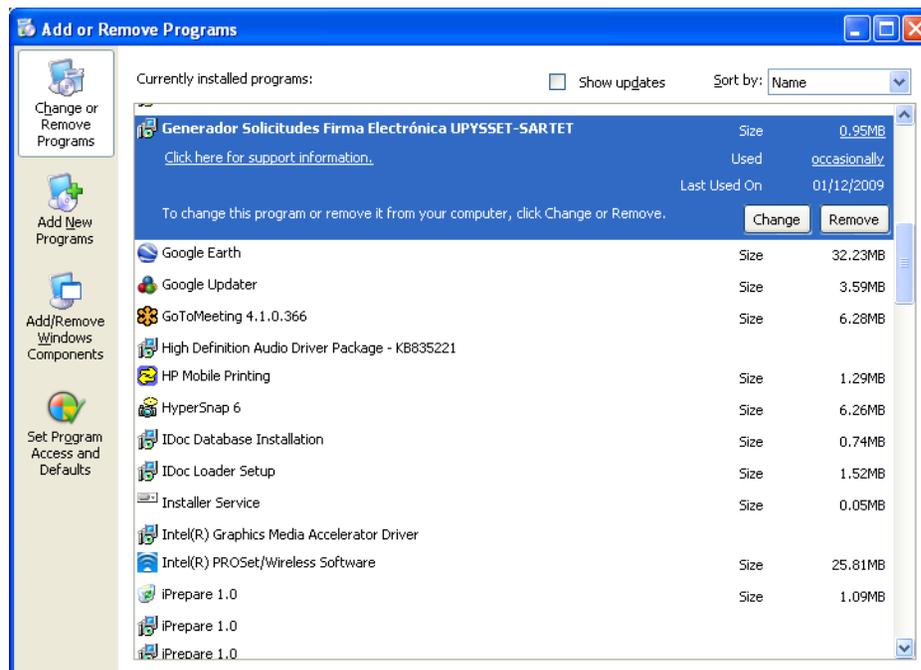


Figura 0-2 Agregar o quitar programas

De la lista de programas, seleccionar “Generator Solicitudes Firma Electrónica IPSSSET-SARTET” y presionar el botón de Quitar. Aparecerá el siguiente mensaje de confirmación:

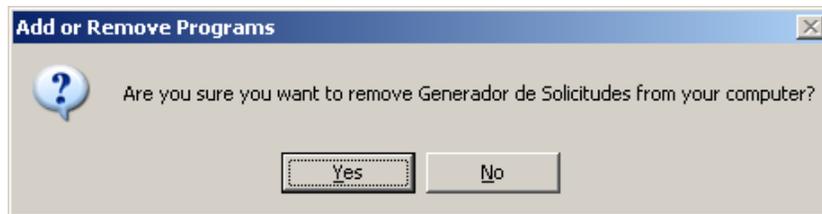


Figura 0-3 Confirmación de desinstalación

Y al dar clic en "Si", se desinstalará el programa.