

**GDE**

**Gestión Documental Electrónica**



# FIRMA DIGITAL CON TOKEN



**Dirección Nacional  
de Gestión Territorial**  
Secretaría de Modernización Administrativa



**Ministerio de Modernización  
Presidencia de la Nación**

## CONTENIDOS

<b>1. Objetivos del Documento.....</b>	<b>1</b>
<b>2. Pre-condiciones .....</b>	<b>2</b>
<b>3. Instalación del Dispositivo.....</b>	<b>3</b>
<b>4. Instalación de Aplicativos.....</b>	<b>5</b>
4.1 Mozilla Firefox.....	5
4.2 Google Chrome .....	9
<b>ANEXO I: Configuración JAVA .....</b>	<b>13</b>
-Precondiciones.....	13
-Procedimientos .....	13
<b>ANEXO II: Instalación de Certificados para validar firmas en PDF.....</b>	<b>16</b>
-Instalación Certificado AC-RAIZ de Firma Digital .....	16
<b>ANEXO III: Configuración de TOKEN USB para firma en lote.....</b>	<b>19</b>
-Procedimiento .....	19
<b>GLOSARIO .....</b>	<b>22</b>

---

## 1. OBJETIVOS DEL DOCUMENTO

---

El presente documento describe el procedimiento para la instalación del dispositivo Criptográfico de Firma Digital (**Token**), necesario para la firma de actos administrativos dentro del módulo **GEDO** de **GDE**.

---

## 2. PRE-CONDICIONES

---

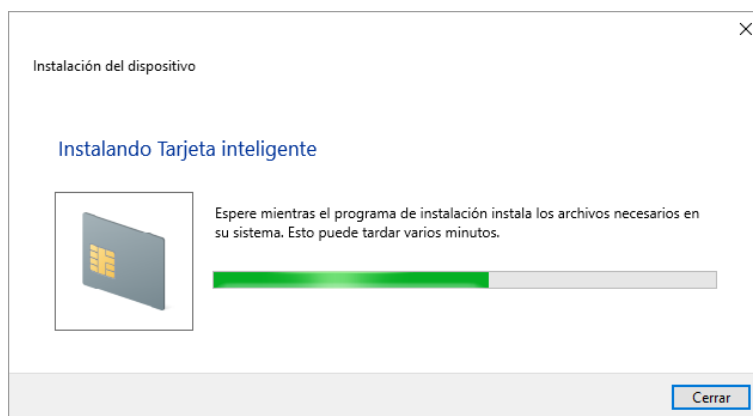
Para seguir correctamente los pasos del presente instructivo es necesario que se cumplan las siguientes precondiciones:

- Se cuenta con el dispositivo de firma digital (**Token**).
- Se cuenta con un usuario y contraseña activos dentro del sistema **GDE**.
- Se cuenta con conocimientos básicos para la utilización de **GDE**.
- Se cuenta con una terminal (PC o Notebook)
  - Con sistema operativo **Microsoft Windows** instalado.
  - Con al menos un puerto USB disponible.
- Se encuentra instalada y configurada la versión Java 1.8.0\_91 o superior en la terminal (ver **ANEXO I: Configuración Java**)
- Se encuentra instalada la aplicación SafeNet Authentication Client (SAC). En caso de no contar con la misma, solicitar el instalador al proveedor del **Token** o bien a la mesa de ayuda.

### 3. INSTALACIÓN DEL DISPOSITIVO

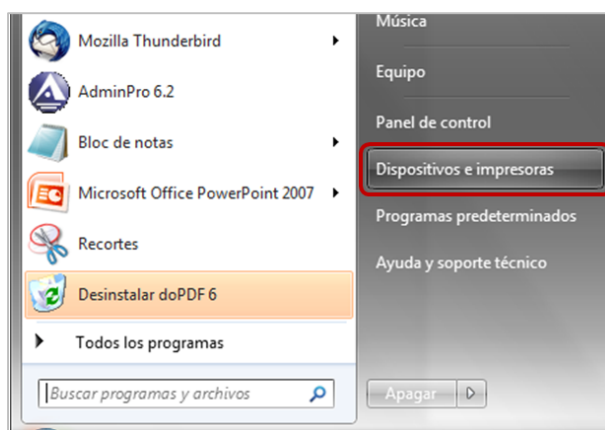
A continuación se detalla paso a paso el procedimiento de instalación:

- 1.1. Insertar el dispositivo **Token** en un puerto USB de la terminal. Windows mostrará una ventana indicando que se ha detectado un nuevo dispositivo e instalará los controladores necesarios. La barra de progreso indicará el porcentaje completado hasta el momento (La imagen puede variar dependiendo la versión de Windows que se encuentre instalada):



- 1.2. Una vez finalizada la instalación de los controladores, la ventana se cerrará automáticamente. Se puede verificar que la instalación se realizó correctamente en la ventana de **Dispositivos e Impresoras**:

- 1.2.1. Windows 7: Presionar el botón **Inicio** -> **Dispositivos e Impresoras**.



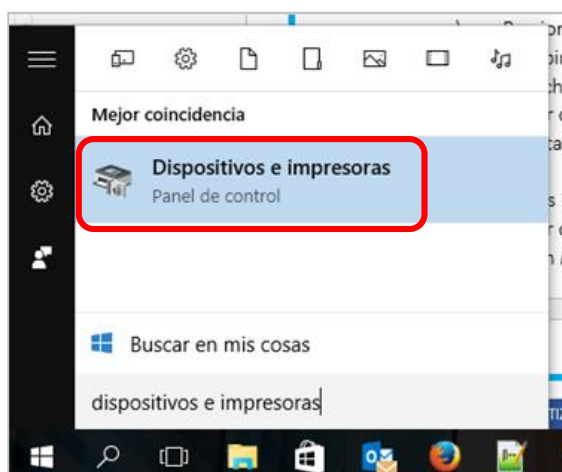
- 1.2.2. Windows 8:

- a. Presionar la tecla Windows.
    - b. Escribir **Dispositivos e impresoras** en el buscador presente en el ángulo superior derecho.

- c. Hacer clic sobre el ícono correspondiente a **Dispositivos e impresoras** en los resultados que aparecen a la izquierda.

#### 1.2.3. Windows 10:

- a. Hacer clic sobre el ícono con una lupa presente en la barra de tareas junto al botón *Inicio*.
- b. Escribir **Dispositivos e impresoras**.
- c. Hacer clic sobre el ícono correspondiente a **Dispositivos e impresoras** en los resultados que aparecen en parte superior.



- 1.3. En todos los casos, se abrirá una ventana similar a la que se puede ver a continuación. Verificar que se encuentre presente en la misma el dispositivo **Token JC**:

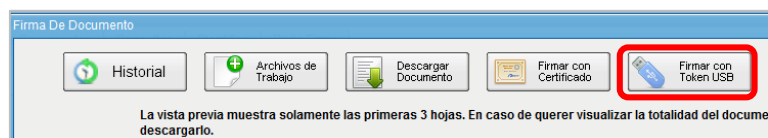


## 4. INSTALACIÓN DE APLICATIVOS

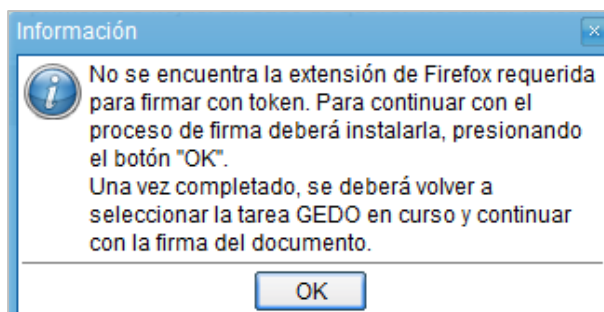
A continuación, se proceden a instalar las extensiones necesarias para los navegadores **Mozilla Firefox** y **Google Chrome**. *(La instalación de ambos navegadores en la terminal es precondition para los pasos que siguen a continuación y está fuera del alcance del presente documento.)*

### 4.1 Mozilla Firefox

- 4.1.1. Generar un documento GEDO y seleccionar la opción para firmarlo [Ver Manual].
- 4.1.2. En la ventana **Firma de Documento** hacer clic sobre el botón **Firmar con Token USB**.



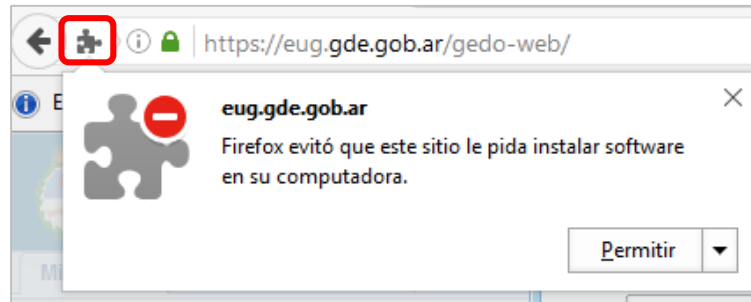
- 4.1.3. El sistema mostrará un cartel informando que no se encuentra instalada la extensión requerida para efectivizar la firma. Hacer clic sobre el botón **OK** para iniciar su instalación.



- 4.1.4. A la izquierda de la barra de dirección del navegador, se desplegará un mensaje emergente solicitando autorización para la instalación de la extensión. Tocar el botón **Permitir**.

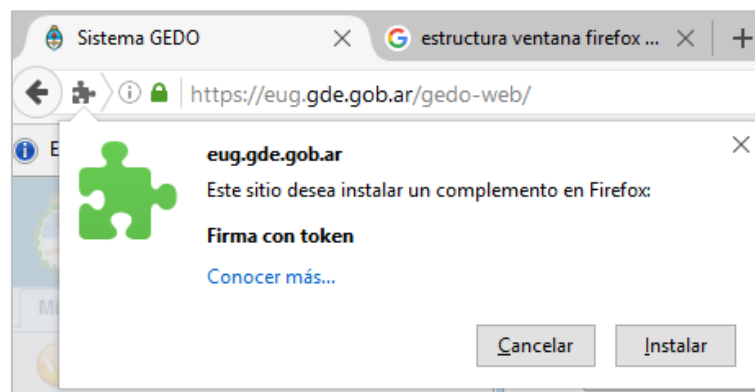
*Nota: Tener en cuenta que si por error se cliquea otro sector de la pantalla, el mensaje emergente quedará oculto y el proceso de instalación no continuará. Para volver a mostrarlo, presionar el ícono con forma de pieza de rompecabezas que se encuentra en el extremo izquierdo de la barra de dirección del navegador.*





4.1.5. Una vez autorizada la instalación, el navegador mostrará nuevamente un mensaje emergente mediante el cual se permite la instalación. Hacer clic sobre el botón **Instalar** para continuar con el proceso.

*Nota: De igual forma que en el paso 4.1.4, presionar el ícono con la pieza de rompecabezas en caso de que el mensaje emergente no se encuentre visible.*



4.1.6. El mensaje cambiará y se mostrará por unos segundos, confirmando que la instalación se realizó correctamente (Imagen 4.1.6.a – Confirmación de instalación Navegador). Adicionalmente, si las notificaciones de escritorio están activas también se mostrará un mensaje en el ángulo inferior derecho de la pantalla (Imagen 4.1.6.b – Notificación de escritorio).

*Nota: De igual forma que en el paso 4.1.4, presionar el ícono con la pieza de rompecabezas en caso de que el mensaje emergente no se encuentre visible.*

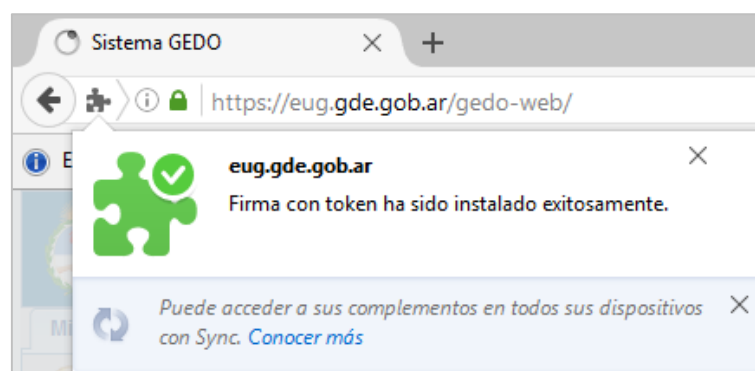


Imagen 4.1.6.a – Confirmación de instalación Navegador

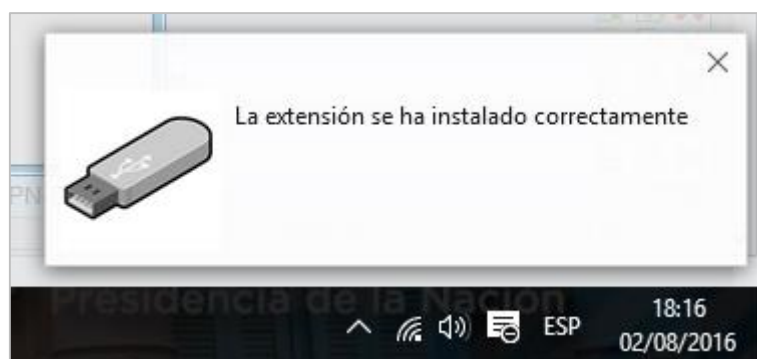
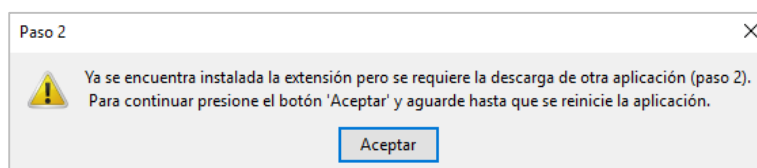
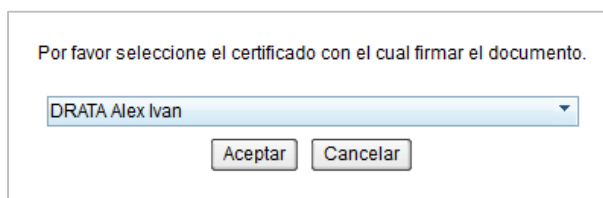


Imagen 4.1.6.B – Notificación de escritorio

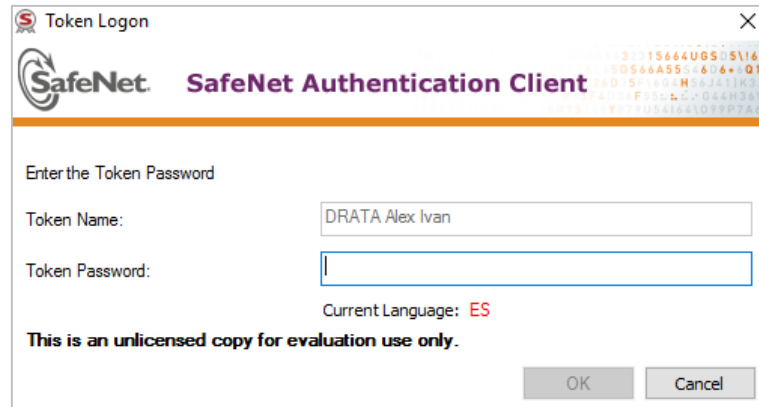
4.1.7. El navegador refrescará la página actual, mostrando nuevamente el listado de documentos. Ejecutar el proceso de firma sobre el registro deseado. Una vez que se llega al punto que se describe en el paso 4.1.2. al hacer clic sobre el botón **Firmar con Token USB** el sistema mostrará el mensaje que se ve en la imagen a continuación. Presionar aceptar para continuar con el proceso:



4.1.8. El navegador descargará otra aplicación y la instalará automáticamente al finalizar (la duración de éste paso puede variar dependiendo la velocidad de conexión). El navegador refrescará la página actual, mostrando nuevamente el listado de documentos. Ejecutar el proceso de firma sobre el registro deseado. Una vez que se llega al punto que se describe en el paso 4.1.2. Al hacer clic sobre el botón **Firmar con Token USB** el sistema mostrará el mensaje emergente con menú desplegable donde debe seleccionarse el certificado con el cual se firmará el documento. Una vez seleccionado, hacer clic sobre el botón aceptar.



4.1.9. El sistema mostrará un nuevo mensaje emergente, solicitando la clave del usuario asociado al **Token** que se encuentra conectado. Ingresarla en el campo **Token Password** y hacer clic sobre el botón **OK**.



Token Logon

**SafeNet** SafeNet Authentication Client

Enter the Token Password

Token Name:

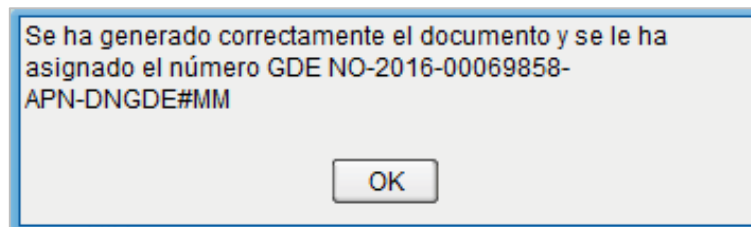
Token Password:

Current Language: **ES**

**This is an unlicensed copy for evaluation use only.**

OK Cancel

4.1.10. Si el dato ingresado es correcto, el proceso de firma finalizará. El sistema mostrará un mensaje emergente informando que se generó correctamente el documento y el número asignado al mismo.

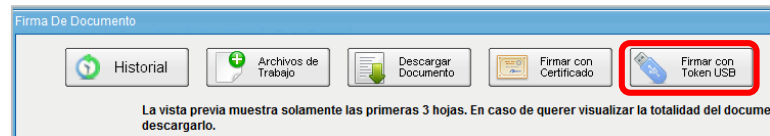


Se ha generado correctamente el documento y se le ha asignado el número GDE NO-2016-00069858-APN-DNGDE#MM

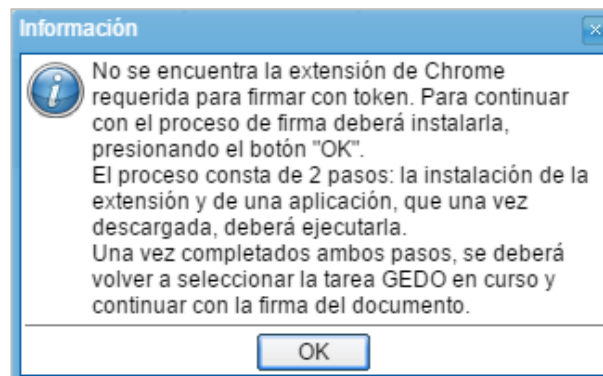
OK

## 4.2 Google Chrome

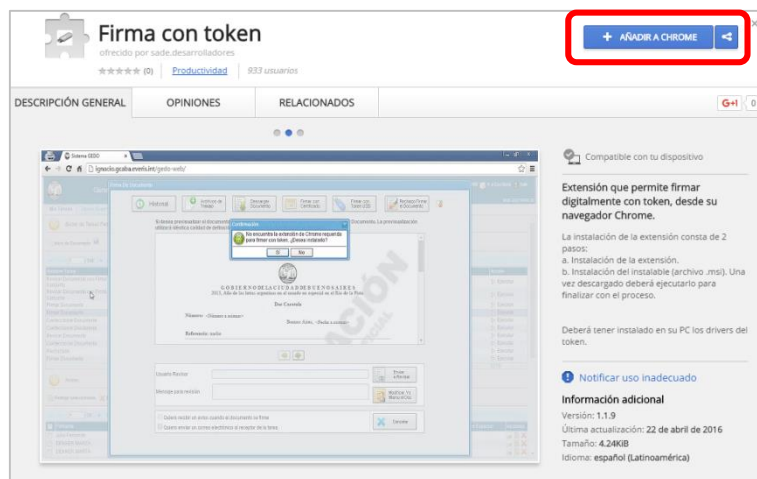
- 4.2.1. Generar un documento GEDO y seleccionar la opción para firmarlo [Ver Manual].
- 4.2.2. En la ventana **Firma de Documento** hacer clic sobre el botón **Firmar con Token USB**.



- 4.2.3. El sistema mostrará un cartel informando que no se encuentra instalada la extensión requerida para efectivizar la firma. Hacer clic sobre el botón **OK** para iniciar su instalación.



- 4.2.4. El navegador será direccionado al sitio Chrome Web Store donde se abrirá la ventana correspondiente a la extensión **Firma con Token**, requerida para continuar. Para instalarla, hacer clic en el botón **+ Añadir a Chrome**, presente en el ángulo superior derecho.



4.2.5. El navegador mostrará un mensaje emergente solicitando autorización para añadir la extensión. Hacer clic sobre botón **Añadir Extensión** (Imagen 4.2.5A – Mensaje emergente de confirmación). El mensaje se cerrará y el botón **+ Añadir a Chrome** cambiará a **Comprobando**. (Imagen 4.2.5B – Transición de estado botón Añadir a Chrome).



Imagen 4.2.5A – Mensaje emergente de confirmación



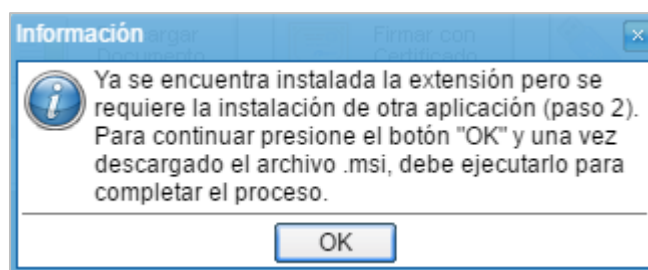
Imagen 4.2.5B – Transición de estado botón Añadir a Chrome

4.2.6. Una vez que finalice la instalación, el botón **Comprobando...** cambiará a **Añadido a Chrome**, de color verde, confirmando que la extensión se instaló correctamente (la duración de éste paso puede variar dependiendo la velocidad de conexión).

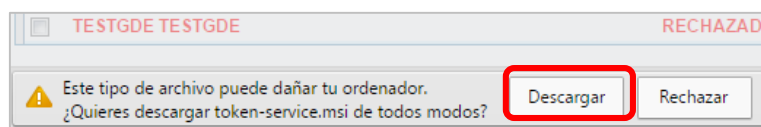


Imagen 4.2.6 – Transición de estado botón Comprobando...

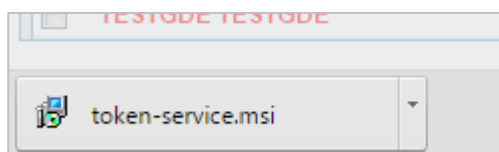
4.2.7. Volver a ingresar al sitio correspondiente al módulo donde se encuentra el documento a firmar ingresando la url en la barra de dirección del navegador. Las credenciales correspondientes al usuario que se encontraba logueado permanecerán activas por lo que se debería ver el listado de documentos disponibles en la grilla **Buzón de tareas pendientes**. Ejecutar el proceso de firma sobre el registro deseado. Una vez que se llega al punto que se describe en el paso 4.2.2. al hacer clic sobre el botón **Firmar con Token USB** el sistema mostrará el mensaje que se ve en la imagen a continuación. Hacer clic sobre el botón **OK** para continuar con el proceso:



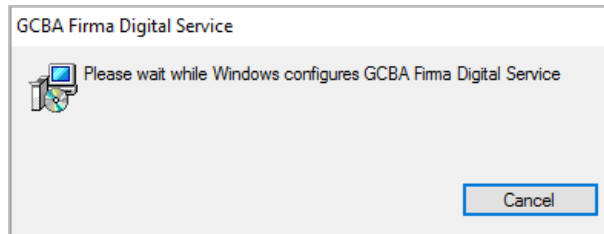
4.2.8. En el ángulo inferior izquierdo de la pantalla el navegador mostrará un mensaje de advertencia, hacer clic sobre el botón **Descargar** para continuar con el proceso:



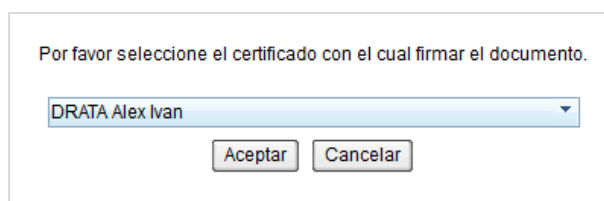
4.2.9. Esperar a que finalice la descarga. El botón cambiará, mostrando el ícono de instalador y el nombre completo (**token-service.msi**). Presionarlo para iniciar la instalación.



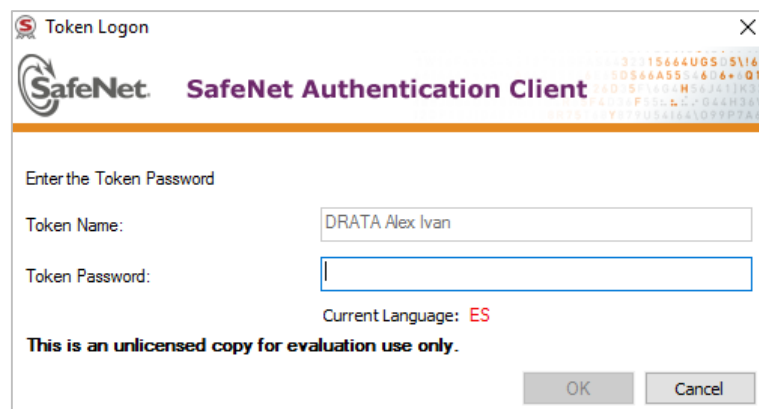
4.2.10. Se abrirá la ventana de instalación del **Servicio Digital de Firma**. El sistema operativo mostrará la ventana de advertencia solicitando confirmación para continuar con la instalación. Hacer clic sobre el botón **Sí** para continuar. La ventana del instalador se cerrará al finalizar.



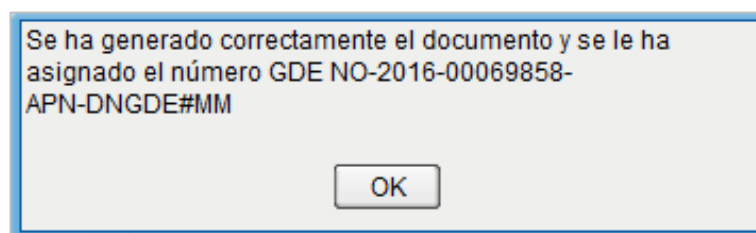
4.2.11. Volver al Navegador **Chrome** y hacer clic sobre el botón **Firmar con Token USB**. El sistema mostrará el mensaje emergente con menú desplegable donde debe seleccionarse el certificado con el cual se firmará el documento. Una vez seleccionado, hacer clic sobre el botón aceptar.



4.2.12. El sistema mostrará un nuevo mensaje emergente, solicitando la clave del usuario asociado al **Token** que se encuentra conectado. Ingresarla en el campo **Token Password** y hacer clic sobre el botón **OK**.



4.2.13. Si el dato ingresado es correcto, el proceso de firma finalizará. El sistema mostrará un mensaje emergente informando que se generó correctamente el documento y el número asignado al mismo.



## ANEXO I: CONFIGURACIÓN JAVA

### Pre-condiciones

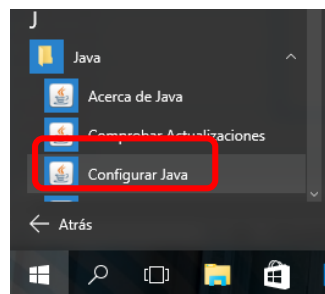
Para seguir correctamente los pasos que se detallan a continuación es necesario que la terminal tenga instalada la versión 8.91 Java JRE

Enlace de descarga:

<http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html>

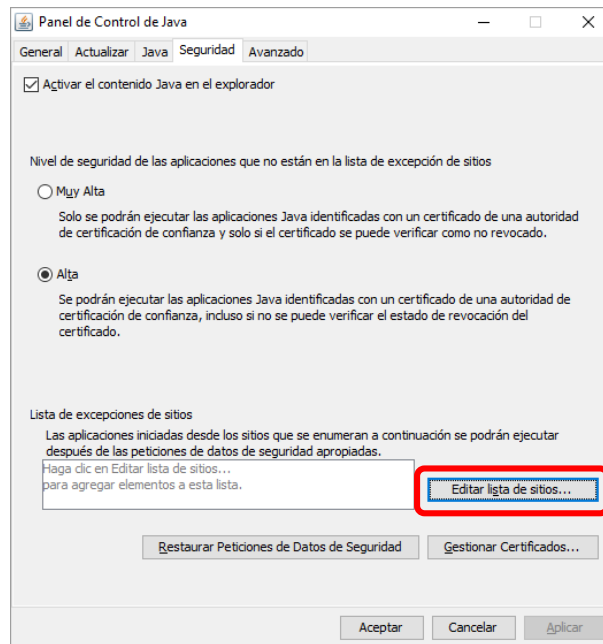
### Procedimiento

- Abrir el Panel de Control de Java en Windows, presionando el botón **Inicio**, submenú **Todas las aplicaciones -> Java -> Configurar Java**.



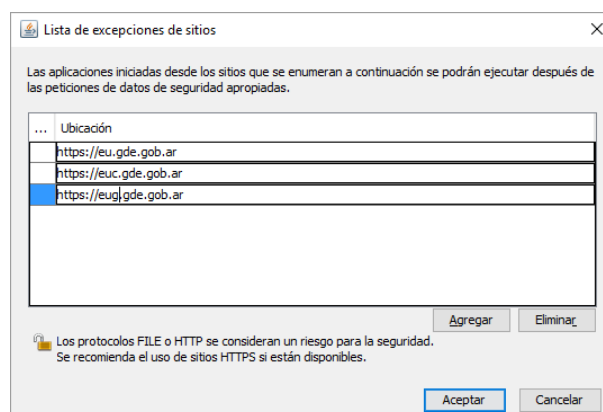
- Hacer clic en la pestaña **Seguridad**. Verificar que se encuentren seleccionadas las opciones
  - a. **Activar el contenido Java en el explorador**.
  - b. **Alta** (Nivel de seguridad)



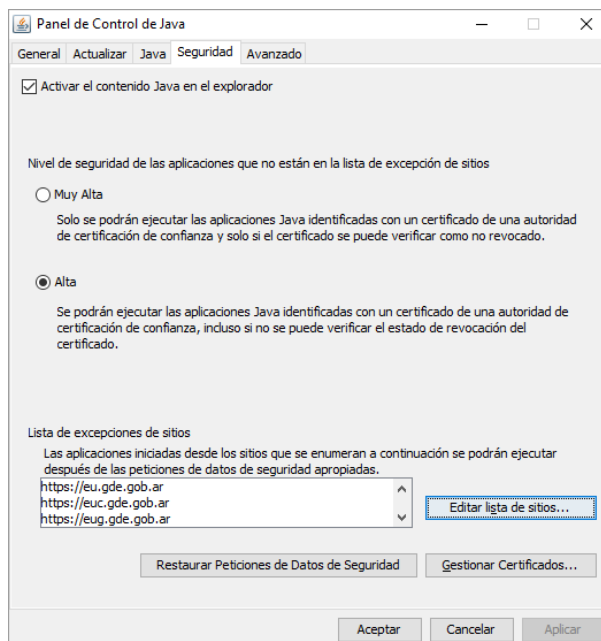


- Hacer clic sobre el botón **Editar lista de sitios**. El sistema mostrará una ventana emergente en la cual se deben agregar los sitios listados en la imagen siguiente. El orden para cargarlos es:
  - a. Hacer clic sobre el botón **Agregar**.
  - b. Escribir la url.
  - c. Hacer clic sobre el botón **Agregar** nuevamente para habilitar un nuevo renglón.

Repetir los pasos hasta que la ventana resultante quede igual que la imagen que se ve a continuación:



- Hacer clic sobre el botón **Aceptar** para volver al panel de control de Java. La ventana debería verse de como la imagen a continuación. Hacer clic sobre el botón **Aceptar** para confirmar todas las configuraciones realizadas:



## ANEXO II: INSTALACIÓN DE CERTIFICADOS PARA VALIDAR FIRMAS EN PDF

### Instalación de Certificado AC-RAIZ de Firma Digital

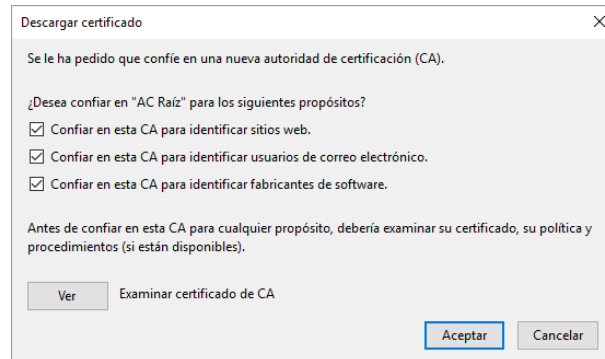
- Abrir el un navegador Mozilla Firefox.
- Ingresar a la siguiente URL: **<https://pki.jgm.gov.ar/app>**
- Hacer clic sobre el botón **Descargue AC-RAIZ**:



- En la siguiente página **Obtener el Certificado Raíz de la Autoridad Certificante**, en la parte inferior, hacer clic sobre el botón **Instalar certificado Raíz**, para descargarlo.



- Se abrirá una ventana emergente en la cual se deben tildar todas las opciones, quedando tal como se ve en la imagen a continuación. Hacer clic sobre el botón **Aceptar** para completar la configuración:



- El mensaje se cerrará y quedará activo el navegador en la página **Obtener el Certificado Raíz de la Autoridad Certificante**, en la parte inferior, hacer clic sobre el botón **Instalar certificado Autoridad Certificante**, para descargarlo.



- Se abrirá una ventana emergente en la cual se deben tildar todas las opciones, quedando tal como se ve en la imagen a continuación. Hacer clic sobre el botón **Aceptar** para completar la configuración:

Descargar certificado

✕

Se le ha pedido que confíe en una nueva autoridad de certificación (CA).

¿Desea confiar en "Autoridad Certificante de Firma Digital" para los siguientes propósitos?

- ☒ Confiar en esta CA para identificar sitios web.
- ☒ Confiar en esta CA para identificar usuarios de correo electrónico.
- ☒ Confiar en esta CA para identificar fabricantes de software.

Antes de confiar en esta CA para cualquier propósito, debería examinar su certificado, su política y procedimientos (si están disponibles).

Ver

Examinar certificado de CA

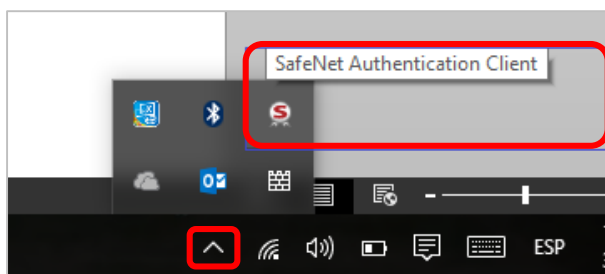
Aceptar

Cancelar

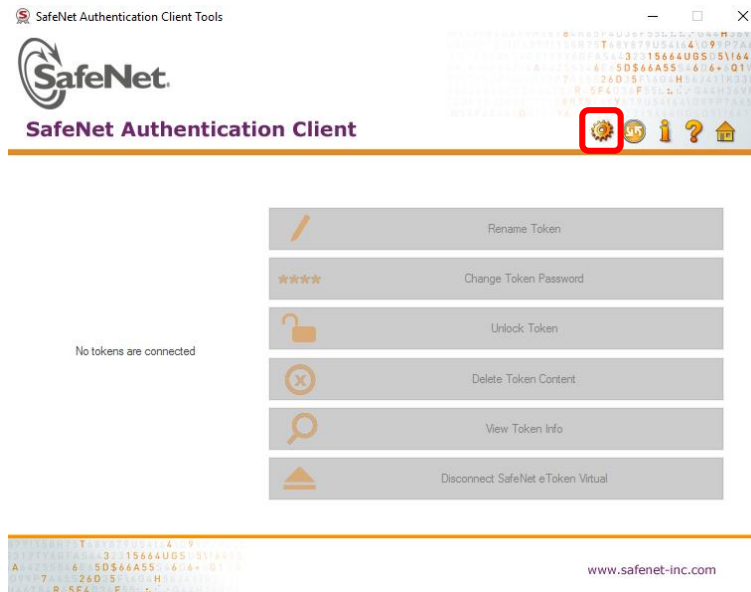
## ANEXO III: CONFIGURACIÓN DE TOKEN USB PARA FIRMA EN LOTE

### Procedimiento

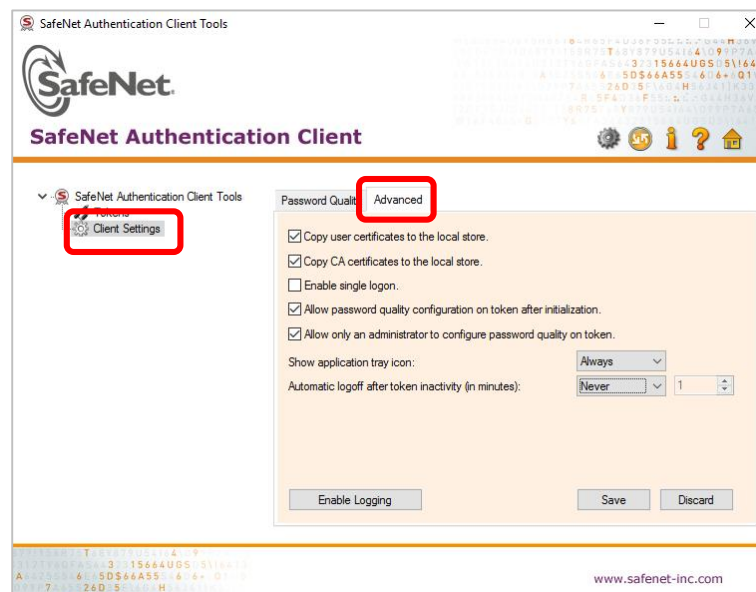
- En la barra de notificación de Windows, situada en el ángulo inferior derecho de la pantalla, verificar que exista el ícono correspondiente al **Safenet Authentication Client**. Es posible que sea necesario presionar el hacer clic sobre el ícono ^ para mostrar los íconos que se encuentran ocultos:



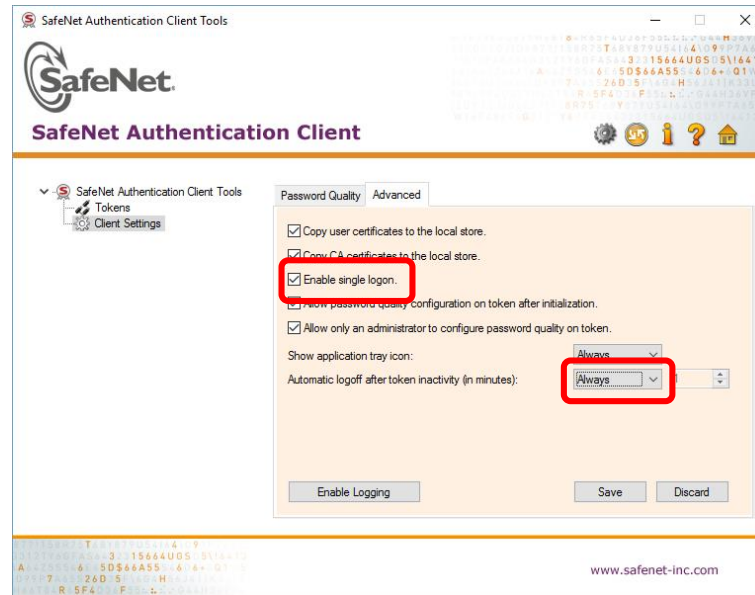
- Hacer doble clic sobre el ícono **Safenet Authentication Client**.
- Se abrirá la aplicación de configuración del **Token**. Hacer clic sobre el ícono representado con un engranaje para acceder a al menú **Advanced View**:



- Dentro de **Advanced View**, hacer clic sobre **Client Settings** presente en el árbol de navegación a la izquierda de la pantalla. Se refrescará el contenido a la derecha de la pantalla:



- Hacer clic en la pestaña **Advanced**.
- Tildar la opción **Enable Single Logon** y en el menú desplegable **Automatic Logoff After Token Inactivity (In Minutes)** seleccionar la opción **Always**.



- Hacer clic sobre el botón **Save** para guardar las configuraciones realizadas.
- Salir de la aplicación.



---

## GLOSARIO

---

- **Autoridad Certificante:** Es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.
- **Algoritmos:** Conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad.
- **Certificado:** Documento informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.
- **Criptográfico:** Que aplica algoritmos para dotar de seguridad a la información.
- **Extensión:** Aplicaciones que agregan nuevas funcionalidades a una aplicación principal. En el caso del presente manual se aplican a los navegadores Google Chrome y Mozilla Firefox.
- **JAVA:** Lenguaje de programación de propósito general.
- **JRE:** *Java Runtime Environment* es un conjunto de utilidades que permite la ejecución de programas Java.
- **Terminal:** PC o Notebook en la cual se está ejecutando la aplicación.
- **Token:** Dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.