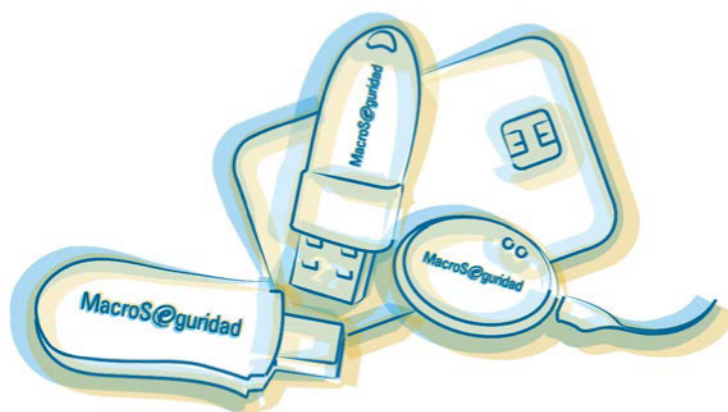


# “Utilizar Mozilla Firefox con los Token USB de Macroseguridad.org”



Nombre del Partner	Mozilla Firefox
Nombre de la Solución	Dispositivos Criptográficos de Macroseguridad (Tokens USB y Smartcards)
Fecha	04 de diciembre de 2017

**Desarrollado por el Departamento IT de Macroseguridad y el Equipo de Integraciones**

#### Revisiones:

Versión	Autor	Fecha	Comentarios
1.0	Santiago Salvatore	13 de Marzo de 2007	1 <sup>er</sup> revisión
1.1	Lionel Raymundi	20 de Marzo de 2007	2da revisión
1.2	Pablo Lloveras	29 de Marzo de 2012	Actualización
1.3	Pablo Lloveras	10 de Septiembre de 2015	Actualización
1.4	Pablo Lloveras	23 de Agosto de 2016	Actualización
1.5	Pablo Lloveras	04 de Diciembre de 2017	Actualización

ADVERTENCIA: Este documento es una guía no oficial para proporcionar un mayor conocimiento para una primera implementación de la solución de seguridad. La información detallada en el mismo es la correspondiente al producto disponible en el mercado a la hora de preparar este documento. Macroseguridad no garantiza que la solución aquí presentada sea completa, adecuada y precisa. Se les recomienda a los usuarios leer los manuales oficiales.

## Tabla de Contenidos

---

<b>A</b>	<b>ACERCA DE MACROSEGURIDAD .....</b>	<b>3</b>
<b>B</b>	<b>INFORMACIÓN DE CONTACTO.....</b>	<b>4</b>
B.1	REDES SOCIALES DE CONTACTO .....	5
<b>C</b>	<b>COPYRIGHT Y MARCAS REGISTRADAS .....</b>	<b>5</b>
<b>D</b>	<b>ACUERDO DE LICENCIA.....</b>	<b>6</b>
<b>1</b>	<b>INTRODUCCIÓN.....</b>	<b>8</b>
1.1	¿QUÉ ES UN TOKEN USB DE MACROSEGURIDAD? .....	8
1.2	¿PARA QUÉ SIRVE UN TOKEN USB DE MACROSEGURIDAD? .....	8
<b>2</b>	<b>ANTES DE COMENZAR.....</b>	<b>9</b>
2.1	INSTALACIÓN DEL MIDDLEWARE DEL DISPOSITIVO CRIPTOGRÁFICO DE MACROSEGURIDAD.ORG (TOKENS USB / SMARTCARD) .....	9
2.2	REQUISITOS.....	9
<b>3</b>	<b>¿QUÉ ES MOZILLA FIREFOX? .....</b>	<b>10</b>
<b>4</b>	<b>INSTALACIÓN DE MOZILLA FIREFOX.....</b>	<b>10</b>
4.1	REQUISITOS PARA LA INSTALACIÓN .....	¡ERROR! MARCADOR NO DEFINIDO.
4.2	COMENZAR LA INSTALACIÓN DE MOZILLA FIREFOX .....	¡ERROR! MARCADOR NO DEFINIDO.
<b>5</b>	<b>CONFIGURANDO LOS DISPOSITIVOS CRIPTOGRÁFICOS DE MACROSEGURIDAD (TOKEN USB / SMARTCARD) EN MOZILLA FIREFOX.....</b>	<b>12</b>
5.1	CARGAR MÓDULO PKCS#11 DE MACROSEGURIDAD .....	13
5.2	INICIAR SESIÓN .....	18
5.3	CAMBIAR CONTRASEÑA.....	19
<b>6</b>	<b>INTEGRACIONES Y APLICACIONES DE LOS TOKENS USB / SMARTCARDS DE MACROSEGURIDAD.ORG .....</b>	<b>20</b>

## A Acerca de Macroseguridad

[MacroSeguridad.org](http://MacroSeguridad.org) es un Mayorista exclusivo de Soluciones de Seguridad Informática, Líder en seguridad digital, y proveedores de seguridad para comercio electrónico e Internet. La compañía atiende a clientes en toda Latino América, México y Brasil.

Macroseguridad cuenta con una experiencia de más de 10 años en el área de seguridad y más de 20 años en el conocimiento y manejo de canales de distribución. Sus consultores y profesionales (Partners, Resellers, Integradores y Partners HI-TECH) demuestran un sólido expertise en los servicios y productos que ofrecen, gracias a un sistema orgánico de capacitación continua tanto en el país como en el exterior, con un amplio conocimiento en diferentes industrias para lograr la diversificación que nuestros clientes necesitan.

Los productos que MacroSeguridad.org distribuye incluyen: [Smartcards](#) (JavaCard, PKI Card), [Lectoras de Smartcards](#) (con conexión USB o interna, con características biométricas, contact y contactless, teclados con biometría y lectoras de smartcards), dispositivos [Tokens USB](#) para firma digital (otorgando portabilidad y transporte seguro de certificados digitales), generando no repudio en comercio electrónico, comunicaciones y Firma Digital. Los [Tokens USB](#) y las Smartcards brindan autenticación robusta y validación de usuarios en los accesos a la red (VPN, SSLVPN, Web Portal). La empresa también comercializa [Tokens OTP](#) (One-Time-Password), dispositivos generadores de números aleatorios para autenticación robusta de usuarios, software para single-sign-on y autenticación. Además, ofrecen soluciones de [Time Stamping](#), [Timbre Digital](#), [Medios de pago](#) diseñados para cumplir con los requerimientos y estándares de Payment Cards y EMV (PCI DSS) y [HSM \(hardware security module\)](#), equipos utilizados para el resguardo y generación de claves privadas. Asimismo ofrecen software para protección de booteo, soluciones de encriptación de archivos y carpetas, logon seguro a la red, seguridad para SAP, autenticación robusta para PDA, teléfonos móviles, etc.

Macroseguridad ofrece [Certificados Digitales SSL](#) para validación de dominios web y protección de datos sensibles en la red, con licencia para ilimitados servidores y compatibles con todos los webservers. Contamos con Certificados SSL para dominio único, certificados Wildcard, multi-dominios y certificados que cumplen con el estándar EV SSL (simple y multi-dominio). También certificados para encriptación y firma digital de correos corporativos y certificados Code Signing (Firma de Código), para la protección de desarrollos distribuidos en la red, que jerarquizan la venta de software vía Internet y evitan los mensajes de error en la descarga on line.

Macroseguridad también distribuye soluciones para la Administración de Derechos Digitales, por ejemplo Dongles - sistemas de protección de software basados en hardware (llaves USB) – para la protección de la propiedad intelectual de los desarrolladores.

Por último, Macroseguridad ofrece soluciones orientadas a los administradores de servidores como UserLock (orientada a robustecer las políticas de seguridad dentro de un Active Directory) y FileAudit (orientada a la auditoría de carpetas y archivos dentro de un File Server).

Macroseguridad Latino América logra el equilibrio entre las necesidades de las empresas y sus soluciones.

Para más información puede visitar [www.MacroSeguridad.org](http://www.MacroSeguridad.org)

## **B Información de Contacto**

Por cualquier consulta, sugerencia o comentario sobre la utilización de la solución o de esta guía, por favor contacte al soporte técnico de Macroseguridad.org

Mail: [suporte@macroseguridad.net](mailto:suporte@macroseguridad.net)

Portal de soporte: <https://suporte.macroseguridad.la>

Web: [www.macroseguridad.net](http://www.macroseguridad.net)

## **B.1 Redes Sociales de Contacto**

Twitter: [@macroseguridad](https://twitter.com/macroseguridad)

LinkedIn: [www.linkedin.com/company/macroseguridad.org](http://www.linkedin.com/company/macroseguridad.org)

WordPress: [macroseguridad.wordpress.com](http://macroseguridad.wordpress.com)

Youtube: [www.youtube.com/Macroseguridad](http://www.youtube.com/Macroseguridad)

## **C Copyright y Marcas Registradas**

COPYRIGHT © 2005-2017

© Este documento es propiedad de Macroseguridad.org y todo su contenido se encuentra protegido por las normas nacionales e internacionales de Derecho de Autor (copyright).

Se encuentra terminantemente prohibida su reproducción total o parcial con cualquier fin. Las marcas mencionadas a lo largo del presente documento son propiedad de sus respectivos titulares.

## D Acuerdo de Licencia

### MacroSeguridad Latino América

#### LEA ATENTAMENTE ANTES DE CONTINUAR CON LA INSTALACIÓN DE SOFTWARE Y/O HARDWARE.

Todos los Productos de Software y/o Hardware que en Latinoamérica son distribuidos por Macroseguridad Latino América (MS Argentina SRL) incluyendo, pero no limitados a, copias de evaluación, diskettes, CD ROMs, hardware y documentación, y todas las órdenes futuras, están sujetas a los términos de este Acuerdo de Licencia y Uso. Si Ud. no está de conforme con los términos aquí incluidos, por favor devuélvanos el paquete de evaluación, empaque y contenido prepago, dentro de los diez (10) días de su recepción, y le reembolsaremos el precio del producto, menos los gastos de envío y cargos incurridos.

1. **Uso Permitido** – Respecto del Software el presente es un acuerdo de Licencia de Uso. Usted no adquiere la propiedad sobre el Software objeto de este Acuerdo sino un Permiso (Licencia) para utilizarlo de conformidad a las siguientes especificaciones. TODOS LOS DERECHOS DE PROPIEDAD INTELECTUAL (incluyendo pero no limitando derechos de autor, secretos comerciales, marcas y patentes) relacionados con el Software, Hardware, sus códigos fuentes, guías de usuario y toda otra documentación comprensiva del mismo son de propiedad exclusiva de Macroseguridad Latino América (MS Argentina SRL) o de las compañías que ésta representa. Ud. puede utilizar este Software únicamente en modo ejecutable, utilizándolo sólo en las computadoras de su empresa u organización, y pudiendo hacer sólo las copias adquiridas en el proceso de compra. En relación al Hardware comercializado por Macroseguridad, usted deberá utilizarlo conforme todas las especificaciones y recomendaciones técnicas informadas. En caso de duda, comunicarnos en el portal de soporte <https://soporte.macroseguridad.la>:

**IMPORTANTE PARA DISPOSITIVOS CRIPTOGRÁFICOS:** Si el dispositivo criptográfico provisto por MACROSEGURIDAD es utilizado apropiadamente y conforme su destino, en el entorno recomendado (Sistema operativo Windows) y con las PASSWORDS correctas, el mismo no bloquea en ningún caso el acceso a la información.

Si esto ocurre, no es por un defecto del producto, sino que, se produce para el resguardo de la información contenida en el dispositivo ante intentos no autorizados o erróneos (por impericia o negligencia del usuario), cumpliendo de esta manera su finalidad.

Se debe tener especial cuidado y precaución en el manejo del dispositivo en el entorno recomendado, así como en el resguardo y respaldo de PASSWORDS de USUARIO y/o ADMINISTRADOR. Al adquirir el producto, el Usuario se compromete a seguir TODAS las recomendaciones técnicas provistas por MACROSEGURIDAD y ante cualquier duda, consultar al equipo de soporte técnico en <https://soporte.macroseguridad.la>

2. **Uso Prohibido** – No puede utilizarse el Software ni el Hardware con otro propósito que el descrito en el apartado 1. El Software o el Hardware o cualquier otra parte del producto no puede ser copiado, realizarse reingeniería, desensamblarse, descompilarse, revisarse, ser mejorado y/o modificado de ninguna otra manera, excepto como específicamente se encuentra admitido en el ítem 1. Ud. no puede utilizar ingeniería inversa en el Software ni en ninguna otra parte del mismo ni intentar descubrir su código fuente. No está permitido tampoco: (1) usar, modificar, fusionar o sublicenciar el Software, salvo lo expresamente autorizado en este contrato; (2) vender, licenciar o sub-licenciar, arrendar, asignar, transferir, comprometerse o compartir sus derechos bajo esta licencia con terceros ;(3) modificar, desensamblar, descompilar, realizar ingeniería inversa, revisar o mejorar el Software o el intento de descubrir el código de fuente del Software; (4) Colocar el Software en un servidor para que sea accesible a través de una red pública; o (5) utilizar cualquier copia de respaldo o archivo del Software (o permitir a otra persona a usar dichas copias) para cualquier propósito distinto del establecido en la presente Licencia.

3. **Garantía** – Se garantiza el Software y el Hardware está sustancialmente libre de defectos significativos en su manufactura o en sus materiales, por el período legal que corresponda contado desde la fecha de entrega del producto conforme factura. La presente garantía no regirá cuando se trate de errores que pueden ser subsanados fácilmente y no implican afectación del rendimiento, cuando los defectos descubiertos hayan sido modificados o alterados sin consentimiento previo del fabricante o cuando el error provenga del mal uso o negligencia o defectos en la instalación. El reclamo deberá realizarse por escrito durante el período de garantía y dentro de los 7 siete días de la observación del defecto acompañado de prueba de los errores detallados. Cualquier producto que Ud. devuelva al fabricante o a un distribuidor autorizado de Macroseguridad deberá ser remitido con el envío y el seguro prepago.
4. **Incumplimiento de la Garantía** – Para el caso de incumplimiento de esta garantía, Macroseguridad Latino América podrá reemplazar o reparar, a discreción del fabricante y con cargo al adquirente /usuario, cualquiera de los productos involucrados.

**CON EXCEPCION DE LO DISPUESTO EXPRESAMENTE EN EL PRESENTE, NO EXISTE NINGUNA OTRA GARANTIA O REPRESENTACIÓN DEL PRODUCTO, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITADA A, CUALQUIER GARANTIA IMPLICITAS DE COMERCIALIZACIÓN Y/O ADAPTABILIDAD PARA UN PROPÓSITO PARTICULAR.**

5. **Limitación de la Garantía del fabricante y/o Macroseguridad** – La responsabilidad total del fabricante frente a cualquier persona o causa, sea contractual como extracontractualmente, incluyendo negligencia o dolo, no podrá exceder el precio de la unidad de producto por Ud. pagado que ha causado el daño o resulta ser el objeto que directa o indirectamente se encuentra relacionado con el hecho dañoso. En ningún caso Macroseguridad Latino América o el fabricante serán responsabilizados por cualquier daño causado por un acto ajeno, impropio, o negligente en el uso del producto, o el incumplimiento de las obligaciones en el presente asumidas, así como tampoco, por la pérdida de cualquier información, dato, ganancia o ahorro, o cualquier otro daño consecuente o incidental, incluso si el fabricante y/o Macroseguridad Latino América hubiese sido advertido de la posibilidad de daño.
6. **TERMINACIÓN DEL ACUERDO DE LICENCIA.** El Acuerdo se considerará terminado frente al incumplimiento de los términos a su cargo. Al término de este contrato expirará la Licencia otorgada y deberá suspender todo uso posterior del Software, y borrar o eliminar cualquier información vinculada al mismo y de propiedad del fabricante. Los ítems 2, 3, 4 y 5 se mantendrán a pesar de la finalización del acuerdo.

## 1 Introducción

### 1.1 ¿Qué es un Token USB de Macroseguridad?

Los Tokens USB de Macroseguridad.org son dispositivos de autenticación de usuarios y portabilidad de certificados digitales, plug and play, ligeros, portátiles, pequeños, que proveen la mejor seguridad al menor costo y que se conectan al puerto USB (Universal Serial Bus) de cualquier PC. Para trabajar con los tokens usb no se requiere ninguna fuente de energía adicional, ni se requiere lectora, ni ningún otro tipo de dispositivo.

### 1.2 ¿Para qué sirve un Token USB de Macroseguridad?

Es la solución para poder transportar su identidad digital que le permite al usuario almacenar su certificado digital en un dispositivo físico (smartcard usb) altamente seguro. De esta forma sus credenciales pueden ser transportadas de una PC a otra sin perder la seguridad, integridad y confiabilidad que Macroseguridad.org le brinda a través de su mecanismo de autenticación de doble factor o triple factor: algo que tengo físicamente, un "Token USB de Macroseguridad", y algo que conozco que es "la password del Token" y quien soy (ADN, Iris, Biometría, etc) brinda el tercer Factor de Autenticación.



## 2 Antes de Comenzar

### 2.1 Instalación del middleware del Dispositivo Criptográfico de Macroseguridad.org (Tokens USB / Smartcard)

Para poder utilizar un Token USB / SmartCard de Macroseguridad deberá tener [instalado el middleware del mismo](#). De no ser así por favor instálelo y luego siga con esta guía. Podrá obtener una guía de instalación del middleware en el siguiente vínculo:

[www.macroseguridad.net/docs](http://www.macroseguridad.net/docs)

El middleware del dispositivo criptográfico de Macroseguridad.org incluye todos los drivers necesarios para que su sistema detecte automáticamente el dispositivo (sea un Token USB o una Smartcard) y le permita descargar sus certificados directamente al mismo, además contiene una importante herramienta para el uso del dispositivo, el *Administrador de Certificados*. Esta herramienta le permitirá cambiar el PIN que viene por defecto por otro que usted desee, cambiar el nombre del dispositivo para poder identificarlo con mayor facilidad, y poder exportar e importar certificados desde y hacia el dispositivo así como también eliminarlos.

### 2.2 Requisitos

- ✓ IDProtect Client 7.12.16 o superior.
- ✓ Middleware y herramientas del Token USB / Smartcards instaladas.
- ✓ Sistemas Operativos: Windows XP SP3, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003., Windows Server 2008, Windows Server 2012, Windows Server 2016 o superior.
- ✓ Puerto USB habilitado o Lectora de SmartCards lista para funcionar.
- ✓ Un dispositivo criptográfico de Macroseguridad listo para usar.

Las capturas en esta guía se realizaron bajo la plataforma **Windows 10 de 64 bits** junto con **Mozilla Firefox**.

### 3 ¿Qué es Mozilla Firefox?

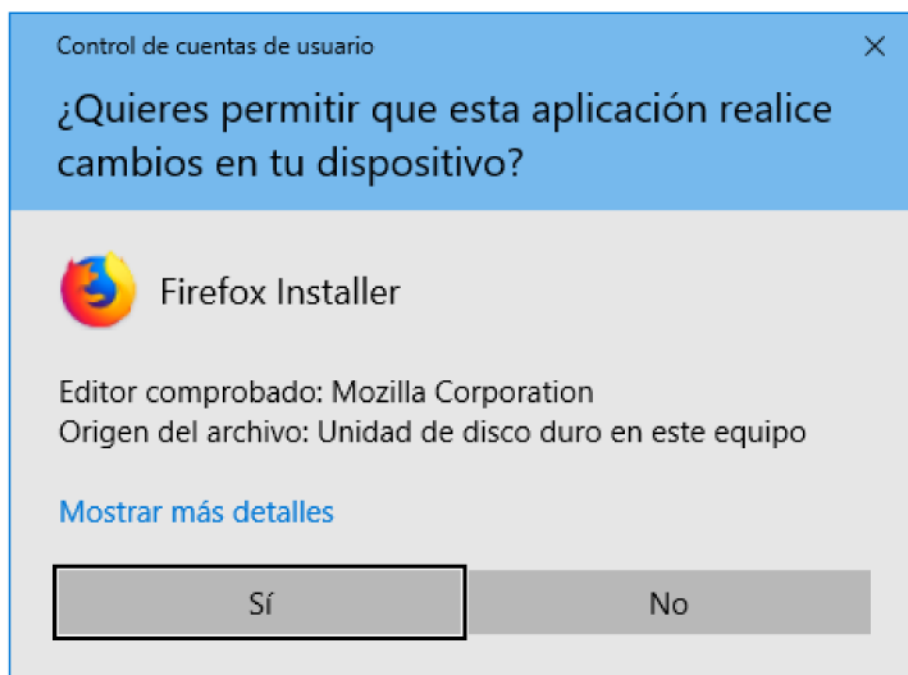
Mozilla Firefox es un navegador de Internet, con interfaz gráfica de usuario desarrollado por la Fundación Mozilla y un gran número de voluntarios externos.

El código fuente de Firefox está disponible bajo la licencia MPL, GNU GPL o GNU LGPL como un programa libre y de código abierto.

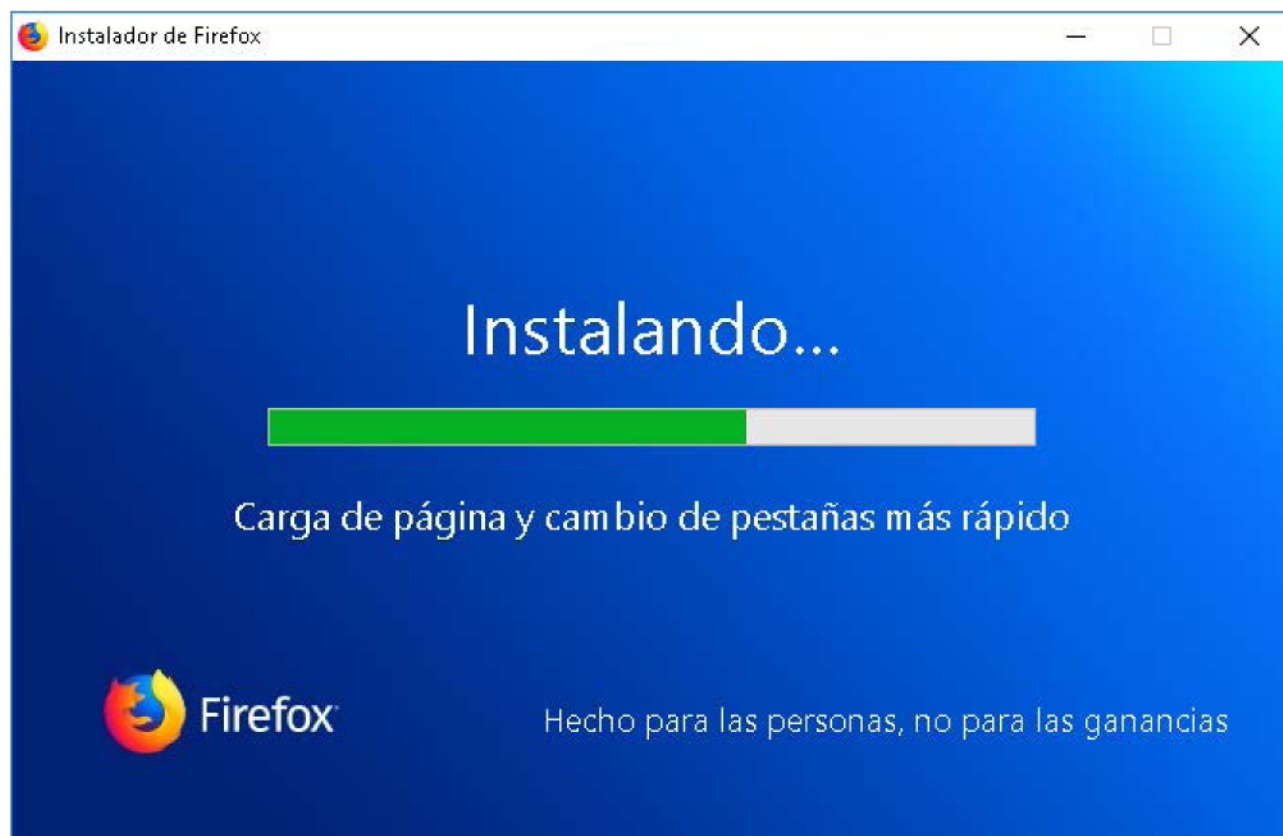
### 4 Instalación de Mozilla Firefox

El software es gratuito y se puede descargar de la página oficial de Mozilla <https://www.mozilla.org/firefox/new/>.

Una vez descargado el archivo de instalación, ejecútelo. Windows le preguntará si desea ejecutar el archivo. Haga click en “Sí” para continuar.



El asistente de instalación comenzará a instalar Mozilla Firefox automáticamente



Una vez finalizada la instalación, se abrirá Mozilla Firefox automáticamente. Podrá seleccionar si desea importar sus opciones, favoritos, historial, contraseñas y otros datos, de algún otro navegador que tenga instalado en su PC. Caso contrario seleccione "No importar nada". Luego le preguntará si desea que Mozilla Firefox sea el navegador web predeterminado. Seleccione la opción que usted prefiera. Ahora tendrá instalado Mozilla Firefox en su equipo.

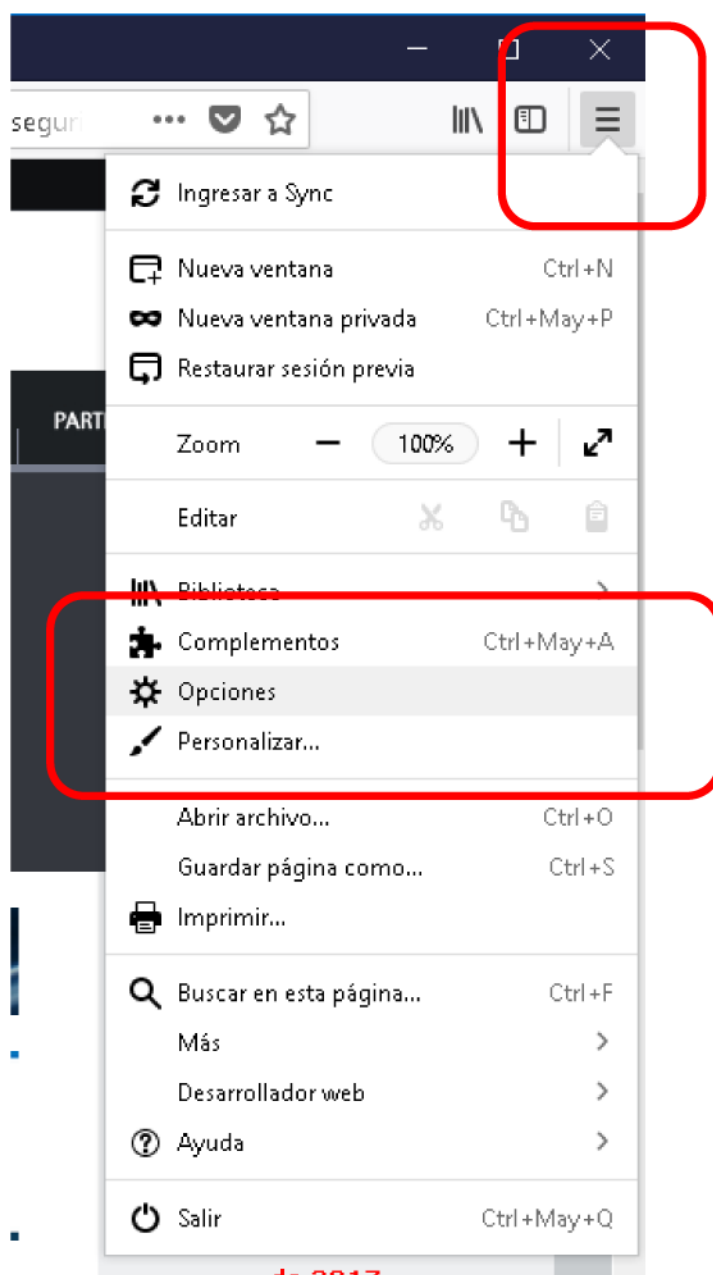


## 5 Configurando los dispositivos criptográficos de Macroseguridad (Token USB / Smartcard) en Mozilla Firefox

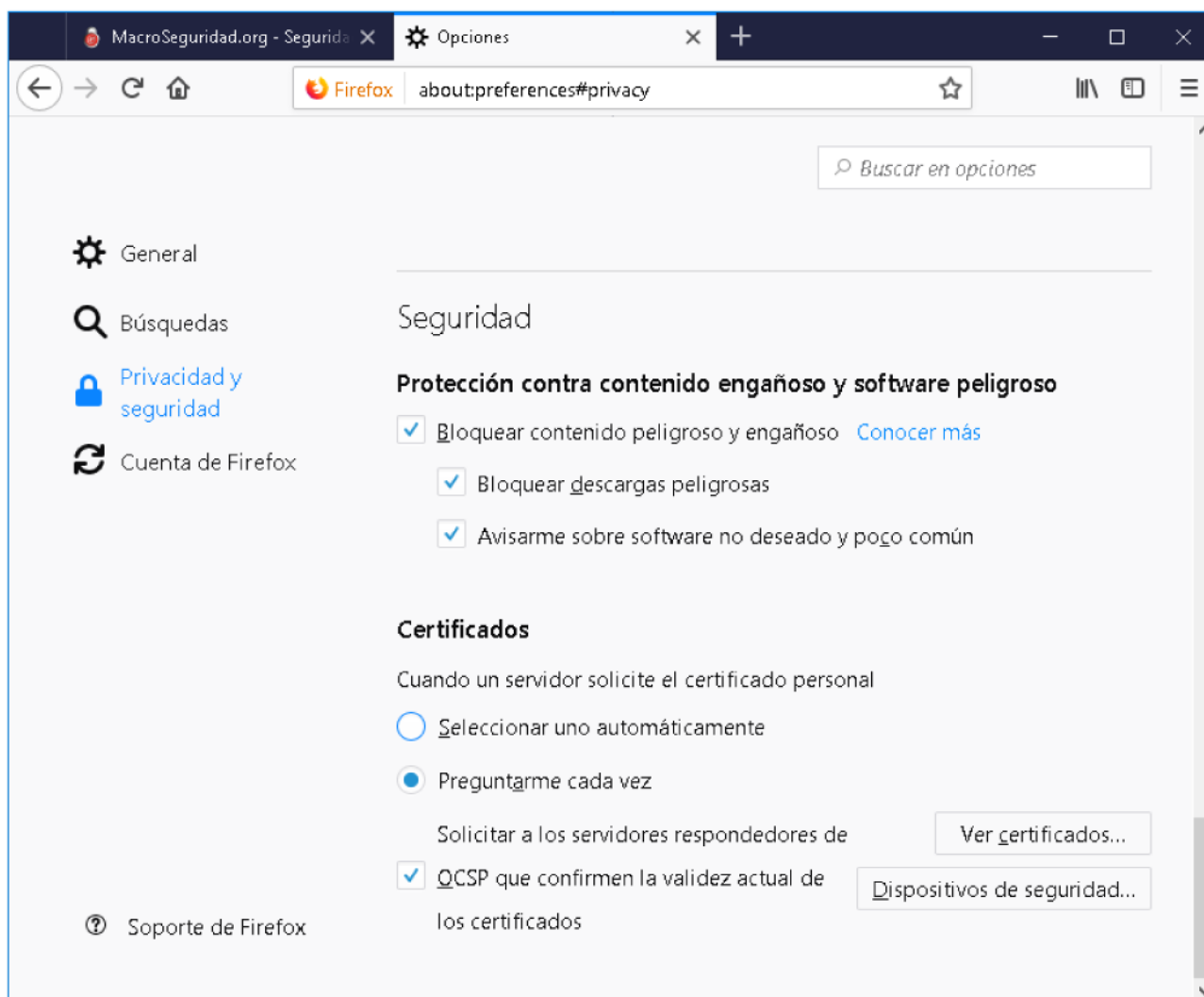
Para poder configurar los Token USB o Smartcards de Macroseguridad en Mozilla Firefox debe tener instalado el Middleware del dispositivo, y el navegador Mozilla Firefox. De no ser así por favor instálelo y luego siga con esta guía. Puede obtener una guía de instalación del middleware correspondiente al producto en su poder lo invitamos a que visite el siguiente vínculo: [www.macroseguridad.net/docs](http://www.macroseguridad.net/docs).

## 5.1 Cargar Módulo PKCS#11 de Macroseguridad

En la barra de herramientas de Mozilla Firefox, que se encuentra en la parte superior, haga click sobre el botón de menú y luego sobre “Opciones” como muestra a continuación.



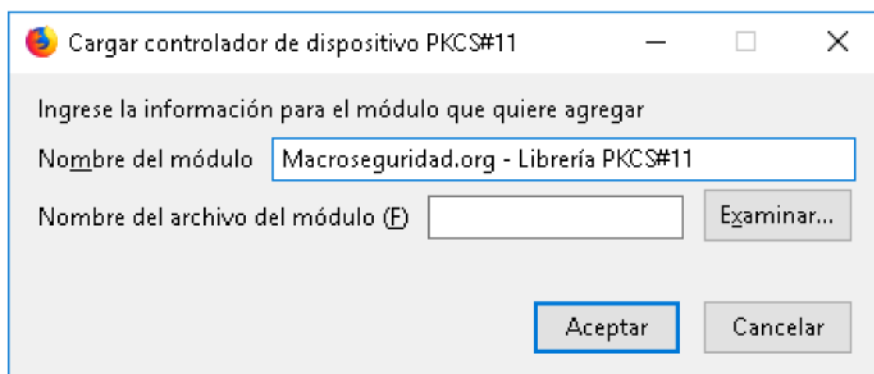
Haga click sobre “Privacidad y seguridad” y luego sobre “Dispositivos de seguridad...”.



Se mostrará la ventana de administrador de dispositivos:

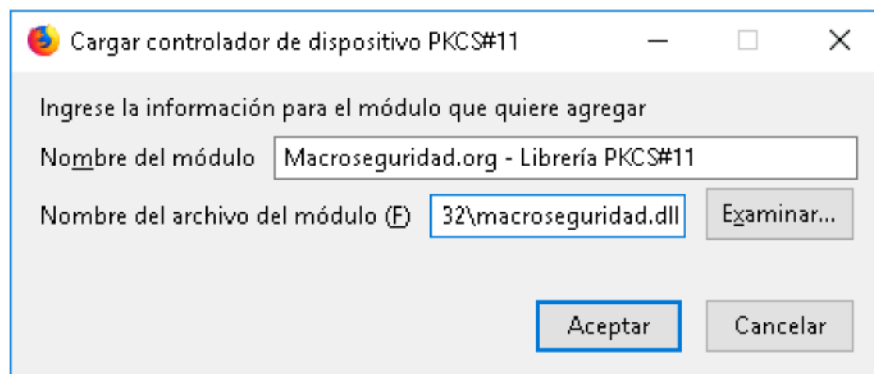


Haga click en el botón “Cargar”. Se mostrará la siguiente ventana. Ingrese un nombre para el módulo que va a instalar, por ejemplo “*Librería PKCS#11 Macroseguridad*”.

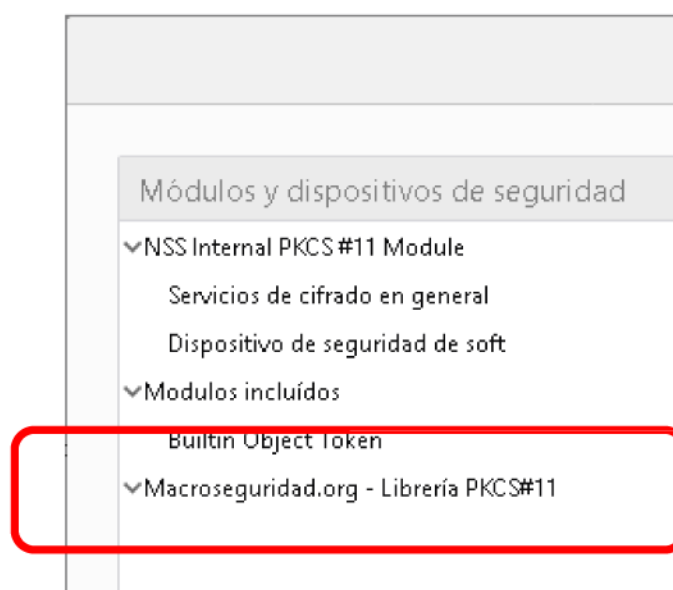


Ahora debe buscar la librería correspondiente a los dispositivos criptográficos de Macroseguridad como ser el Token USB o la Smartcard. Haga click sobre “Examinar...” para seleccionar la librería. En este caso utilizaremos la librería “librería\_pkcs11\_macroseguridad.dll” que se encuentra en la siguiente ubicación: [Unidad de Windows]:\[Capeta de Windows]\system32\.

Refiérase al boletín de compatibilidad PKCS#11 para saber cual es la librería correspondiente a su Token USB / Smartcard. Seleccione la librería correspondiente y luego haga click en “Abrir”. Una vez seleccionada la librería haga Para finalizar la carga del modulo haga click en “Aceptar”.

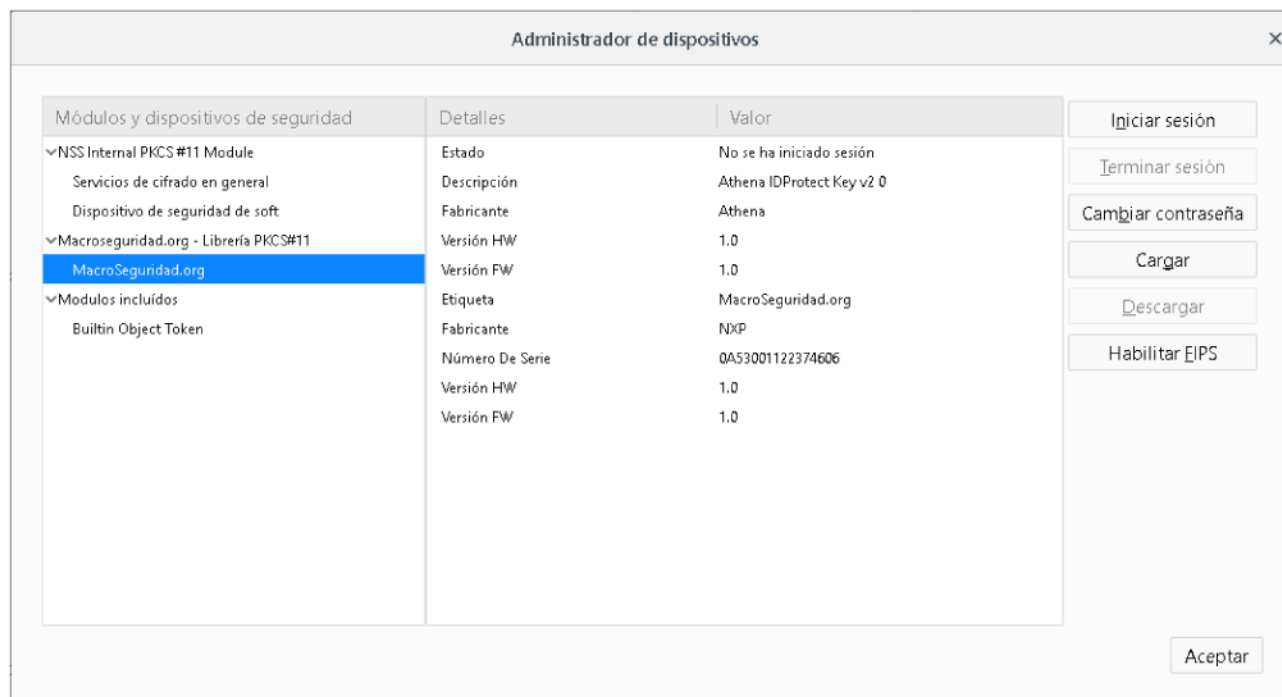


En el Administrador de dispositivos se listará el modulo recientemente configurado.





Si usted conecta un Token USB / Smartcard a su PC la ventana anterior se actualizará y se mostrará de la siguiente forma:

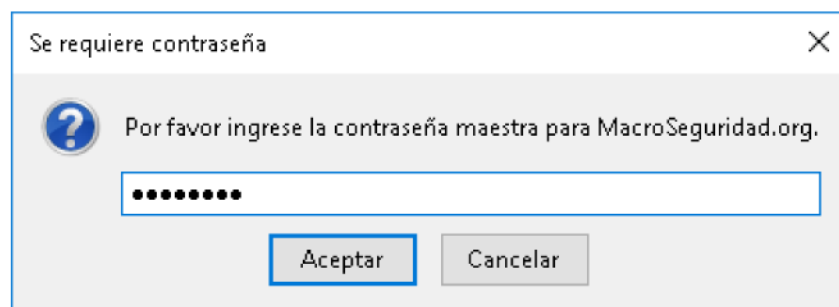


En la parte izquierda se muestran listados los Tokens USB / Smartcards conectados, mostrando el nombre de cada uno. Si se selecciona algún dispositivo, en la parte derecha de la ventana se puede ver la información correspondiente al mismo.

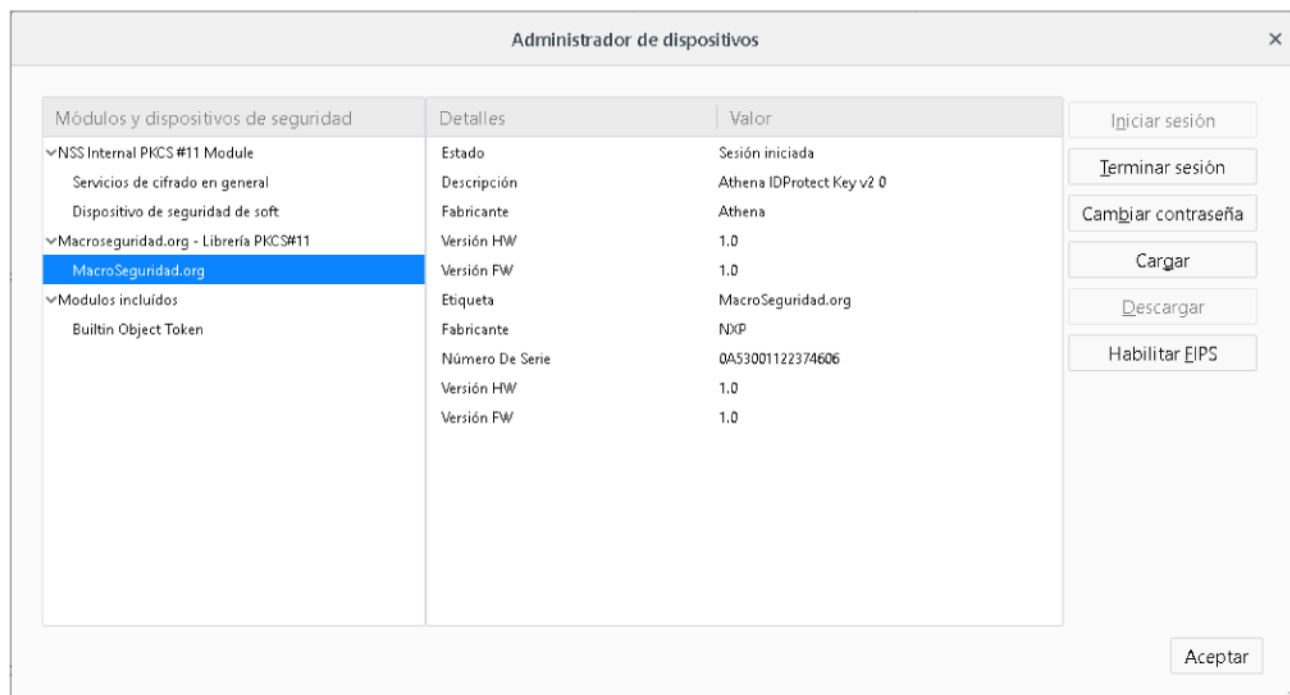
Más a la derecha de la ventana puede observar listadas las operaciones que se pueden realizar con un dispositivo criptográfico de Macroseguridad. Se puede iniciar sesión o cambiar la contraseña del mismo.

## 5.2 Iniciar Sesión

Esta opción sirve para verificar que el modulo criptográfico fue instalado correctamente en Mozilla Firefox. Para iniciar haga click en “*Iniciar sesión*”, luego deberá ingresar el PIN del dispositivo criptográfico.

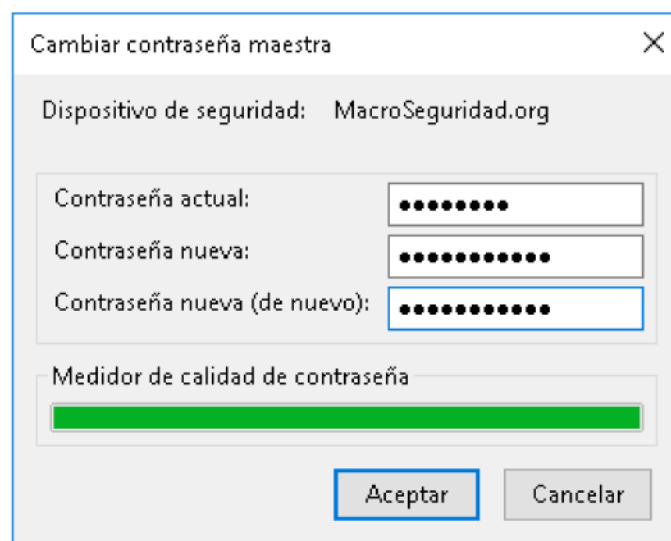


Una vez iniciada la sesión, se deshabilitará el botón de “*Iniciar sesión*”, y se habilitará el de “*Terminar sesión*”, como muestra la siguiente imagen.



## 5.3 Cambiar contraseña

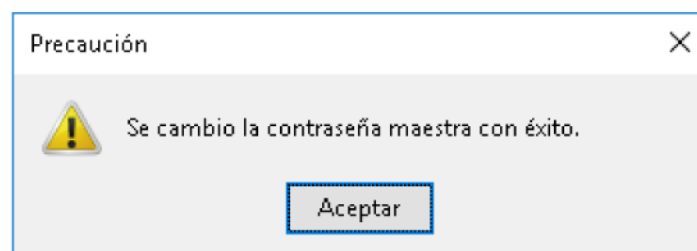
Usted podrá cambiar la contraseña del dispositivo criptografico utilizando Mozilla Firefox. Elija la opción en la parte derecha y una ventana como la siguiente se mostrará:



The screenshot shows a dialog box titled "Cambiar contraseña maestra" with a close button (X) in the top right corner. The text "Dispositivo de seguridad: MacroSeguridad.org" is displayed. Below this, there are three password input fields: "Contraseña actual:" (filled with 10 dots), "Contraseña nueva:" (filled with 10 dots), and "Contraseña nueva (de nuevo):" (filled with 10 dots). Below the input fields is a "Medidor de calidad de contraseña" (password quality meter) shown as a green bar. At the bottom, there are two buttons: "Aceptar" (highlighted with a blue border) and "Cancelar".

Deberá ingresar la contraseña actual por defecto la contraseña del dispositivo criptográfico. Contacte a su Administrador de red para más información.

Luego deberá ingresar el nuevo PIN y la confirmación de la misma. Haga click sobre "Aceptar" para confirmar la operación. Si todos los campos son correctos, se mostrará la siguiente ventana:



The screenshot shows a dialog box titled "Precaución" with a close button (X) in the top right corner. On the left, there is a yellow warning triangle icon. To the right of the icon, the text reads "Se cambio la contraseña maestra con éxito." Below the text is a single button labeled "Aceptar" with a blue border.

## 6 Integraciones y aplicaciones de los Tokens USB / Smartcards de Macroseguridad.org

MacroSeguridad ha desarrollado varias guías de integración para utilizar sus dispositivos criptográficos con las aplicaciones de uso común. Los Tokens USB y SmartCards le permiten robustecer la seguridad de dichas aplicaciones de modo totalmente transparente. Si desea conocer mayor información al respecto de estas guías puede visitar:

<http://www.macroseguridad.net/docs>

Para mayor información o dudas sobre esta guía contacte al equipo de Tecnología de MacroSeguridad.org por el medio que usted prefiera:

- ✉ Mail: [sosporte@macroseguridad.net](mailto:sosporte@macroseguridad.net)
- ✉ Portal de soporte: <https://sosporte.macroseguridad.la>
- ✉ Web: [www.macroseguridad.net](http://www.macroseguridad.net)