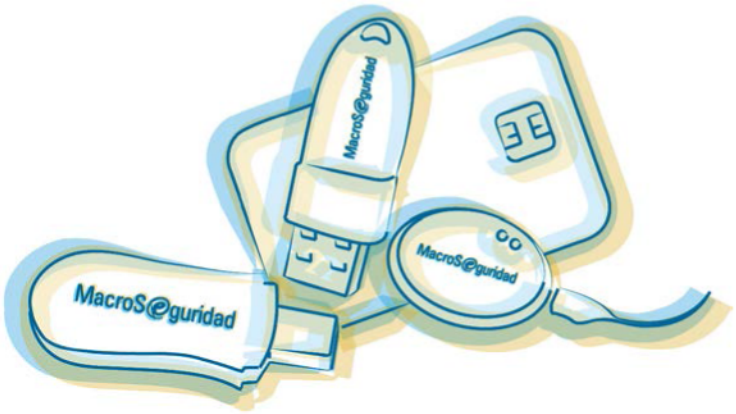
“Guía de instalación del middleware (drivers) de IDProtect”



Nombre del Partner	Athena SmartCard Solutions
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	Pablo Lloveras	18/10/10	Release Inicial
2.0	Pablo Lloveras	01/09/11	Actualización
2.1	Pablo Lloveras	30/09/11	Corrección
3.0	Pablo Lloveras	12/06/15	Actualización y Estructura
4.0	Pablo Lloveras	25/07/16	Actualización
5.0	Pablo Lloveras	04/12/17	Actualización

Tabla de Contenidos

A Acerca de Macroseguridad

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 estandares 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 encripción 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 encripción 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

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 Latino América:

Mail: soporte@macroseguridad.net

Portal de soporte: https://soporte.macroseguridad.la

Web: www.macroseguridad.net

B.1 Redes Sociales de Contacto

Twitter: @macroseguridad

LinkedIn: www.linkedin.com/company/macroseguridad.org

WordPress: macroseguridad.wordpress.com

Youtube: www.youtube.com/Macroseguridad

C Copyright y Marcas Registradas

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, comunicarlas 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 descripto 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 item 1. Ud. no pude 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 items 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 Sistemas operativos soportados

Actualmente **IDProtectClient** soporta las siguientes plataformas:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2012
- Windows 8
- Windows 8.1
- Windows Server 2016
- Windows 10
- Linux
- Mac OS X

Las capturas de esta guía de instalación se realizaron en **Windows 10 de 64 bits**.

2.2 Requisitos mínimos de instalación

Antes de comenzar con la instalación deberá verificar que los siguientes requisitos se cumplan:

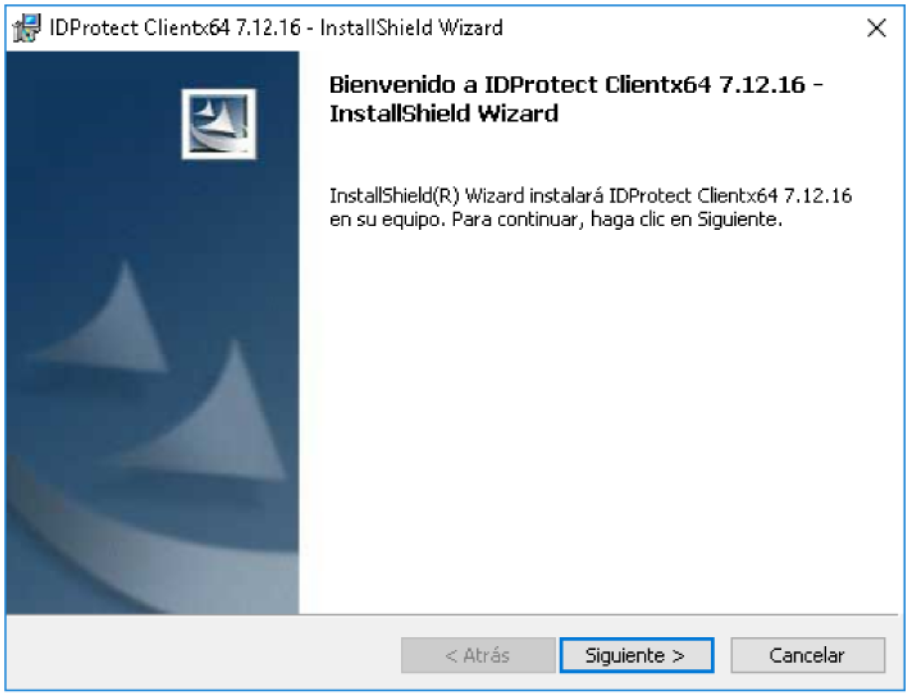
- El sistema operativo es alguno de los mencionados anteriormente.
- Software IDProtectClient 6.40 o superior.
- Permisos de Administrador.
- Un puerto USB disponible.
- Un dispositivo criptográfico de Macroseguridad listo para usar.
- Debe estar habilitado en el MotherBoard el soporte USB.
- Una lectora de SmartCards (Opcional).

3 Instalar el Middleware

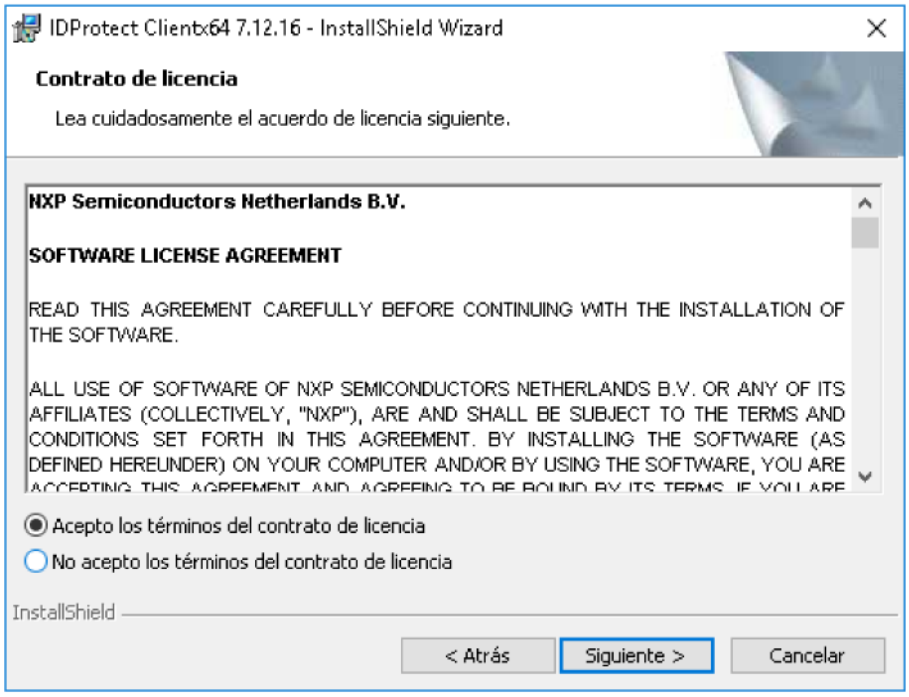
Ud. puede ejecutar "*setup.exe*" dentro la carpeta "*x32*" (para sistemas operativos de 32bits) y "*setup64.exe*" dentro de la carpeta "*x64*" (para sistemas operativos de 64bits). También puede utilizar "*IDProtectClient.msi*" (32bits) o "*IDProtectClientx64.msi*" (64bits) si desea instalar el middleware utilizando la línea de comandos.

Los mismos se encuentran dentro de la carpeta "*Windows\Instaladores_Middleware*" o puede solicitarlos en https://soporte.macroseguridad.la

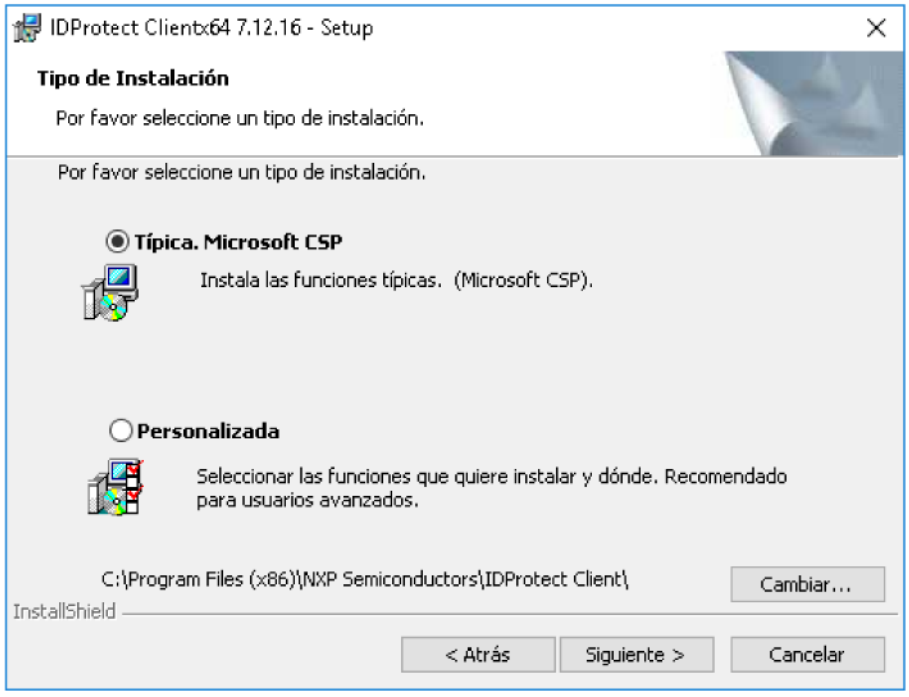
Una vez iniciada la instalación se mostrará el asistente de IDProtect Client. Le informará qué versión del Middleware ud. está por instalar. Para continuar haga click en "*Siguiente >*".



En la siguiente ventana, el asistente mostrará el "*Contrato de licencia*". Para continuar con la instalación debe leer y aceptar el mismo. Selecciona la opción "*Acepto los términos del contrato de licencia*" y haga click en "*Siguiente >*" para continuar.



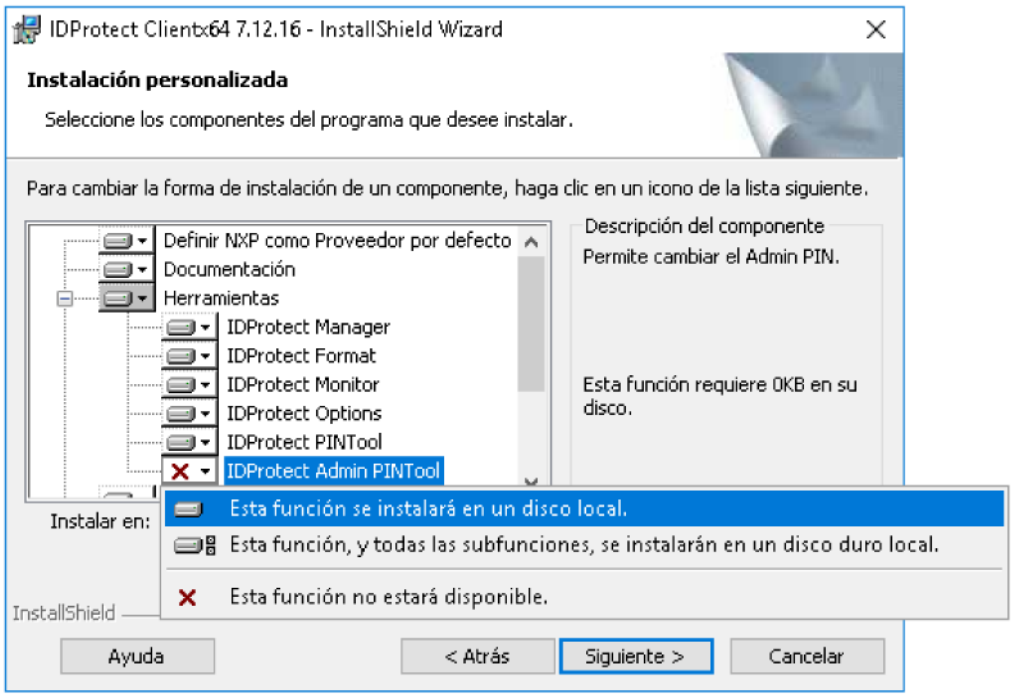
En la siguiente ventana se nos preguntará el tipo de instalación que deseamos realizar. Seleccionaremos "*Típica. Athena CSP*" y hacemos click en el botón "*Siguiente* >".



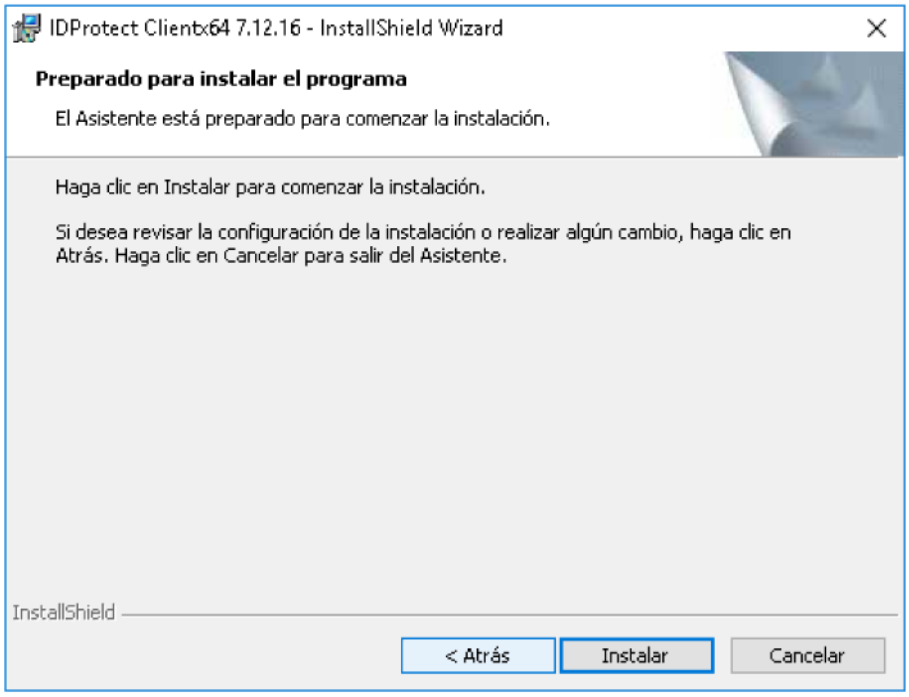
Nota: Si usted posee un Token USB o una Smartcard de Macroseguridad con soporte biométrico deberá:ejecutar el middleware con la siguiente línea de comandos:

```
msiexec /i [ruta al archivo]\IDProtectClient.msi INSTALLCCID=1 INSTBIOCOMP=1
INSTALLBIOTOOL=1 INSTALLPRECISELIBS=1 ASESENSBSPS=16
```

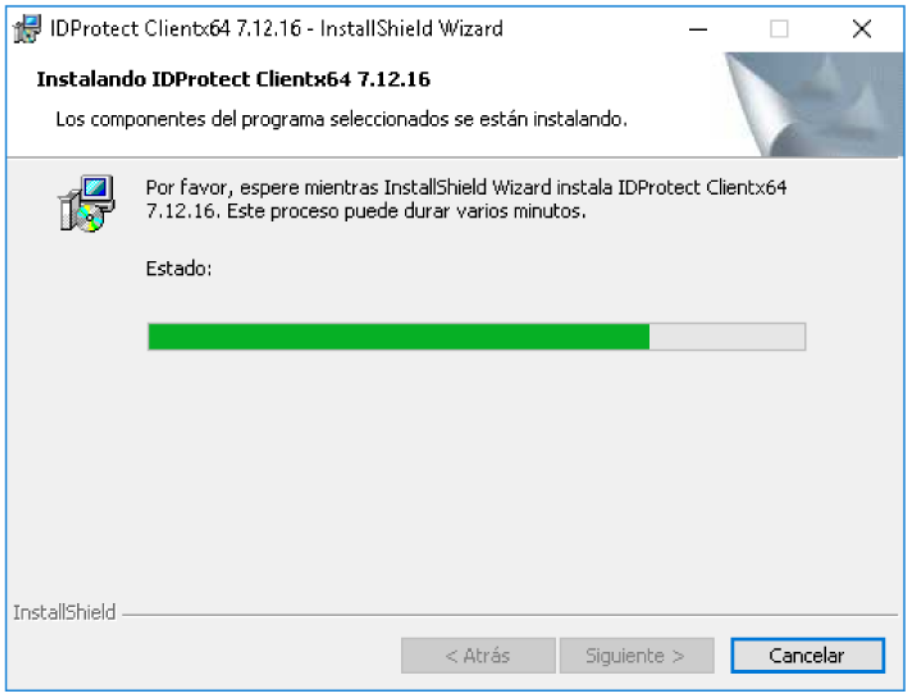
Nota: Si usted desea instalar la herramienta IDProtect Admin PIN deberá seleccionar "*Personalizada*" y luego "*IDProtect Admin PINTool. Esta función se instalará en un disco local.*". Luego haga click en "*Siguiente >*".



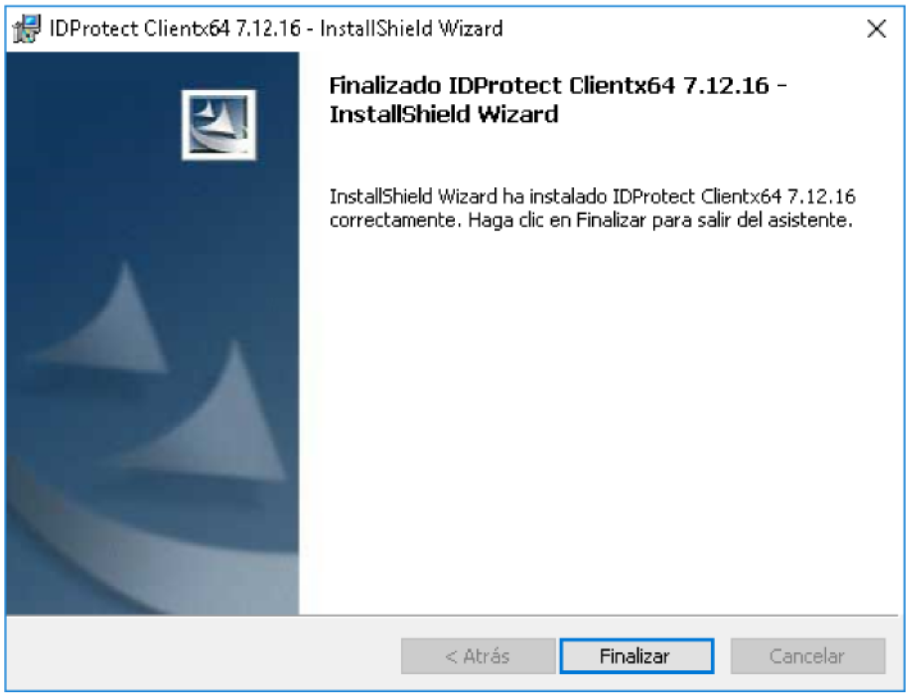
Una vez que que haya determinado los componentes que desea instalar, el asistente le informará que está listo para proceder con la instalación, simplemente haga click en "*Instalar*", para iniciar el proceso de instalación.



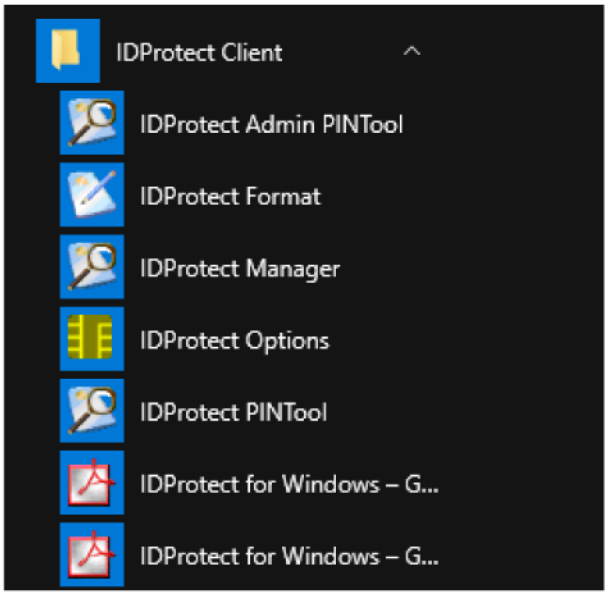
Espere mientas se instala IDProtect Client.



El asistente nos informará que la instalación se realizó con éxito. Para terminar haga click en "*Finalizar*".



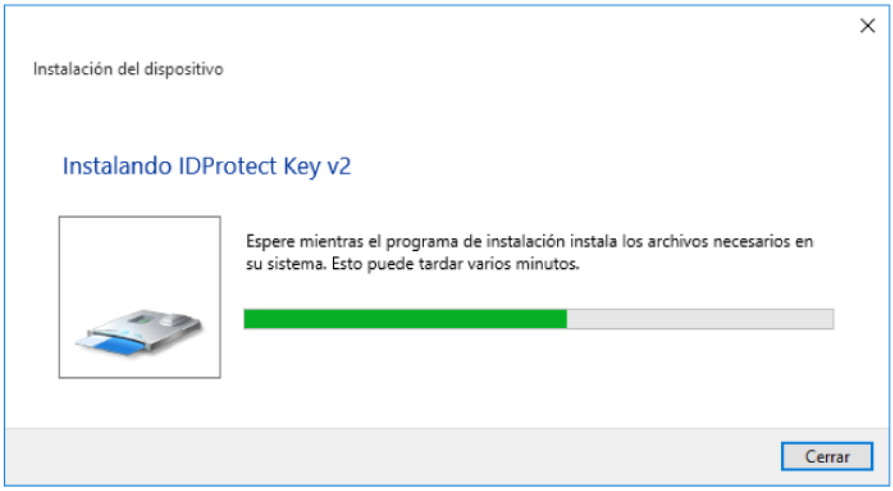
Ahora puede acceder a todas las herramientas instaladas desde el menú de Inicio.



Nota: En caso de que el proceso de instalación se haya interrumpido por algún error, o haya sido cancelado por el usuario, deberá realizar nuevamente todos los pasos de este documento.

Si Mozilla Firefox se encuentra instalado (versión 3.5 o superior) en su equipo, durante la instalación se adicionará el módulo PKCS#11 de MS-IDProtect automáticamente.

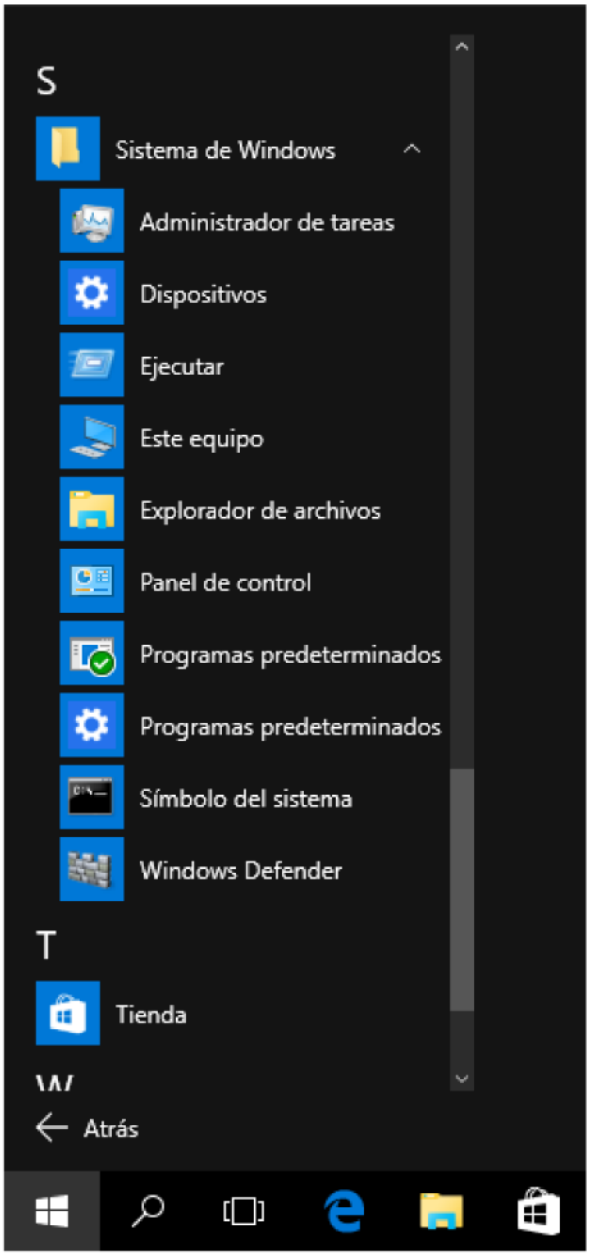
Una vez finalizada la instalación conecte su dispositivo Criptográfico MS-IDProtect. Se mostrará el siguiente diálogo, espere mientras su dispositivo se termina de configurar:



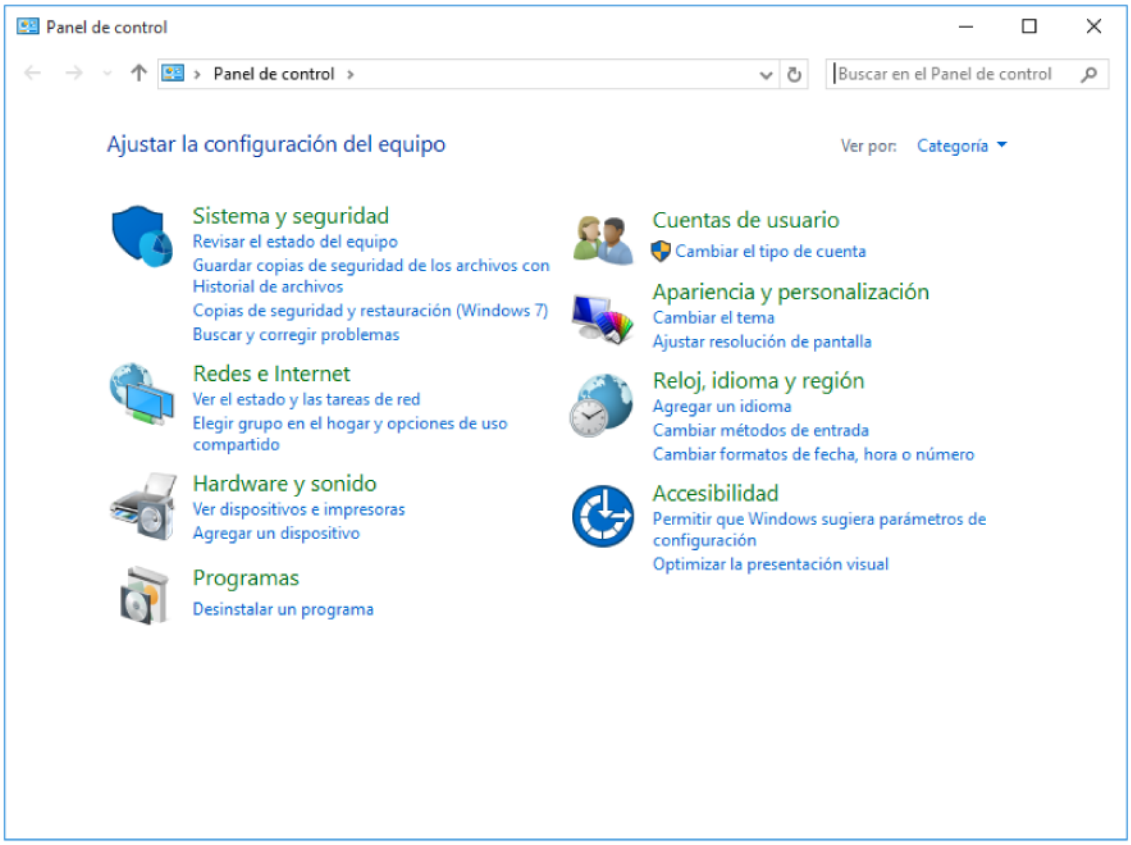
Ahora el dispositivo se encuentra instalado y listo para utilizarse.

4 Desinstalar el Middleware

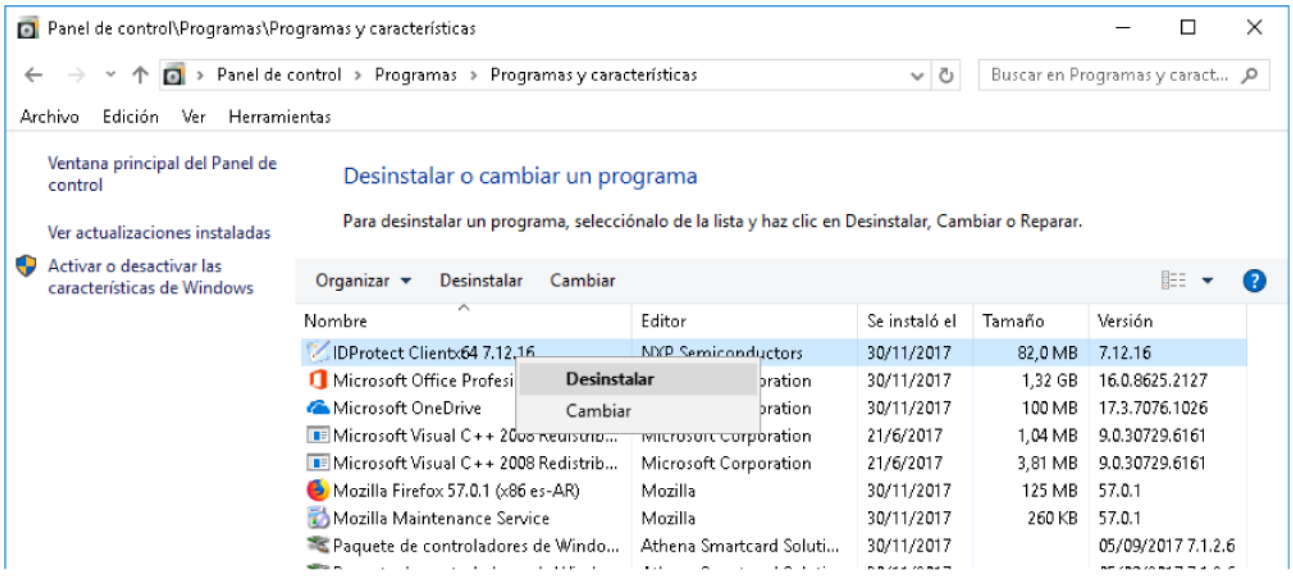
Para desinstalar el middleware IDProtect Client de su equipo diríjase a "*Panel de control*".



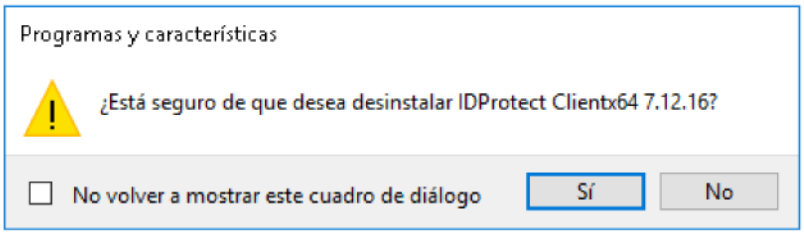
Haga click en "*Desinstalar un programa*".



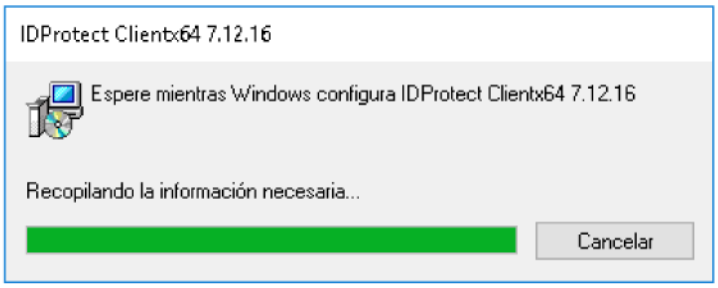
Haga doble click sobre "*IDProtect Client x.xx.xx*" o click con el botón derecho y luego en "*Desinstalar*".



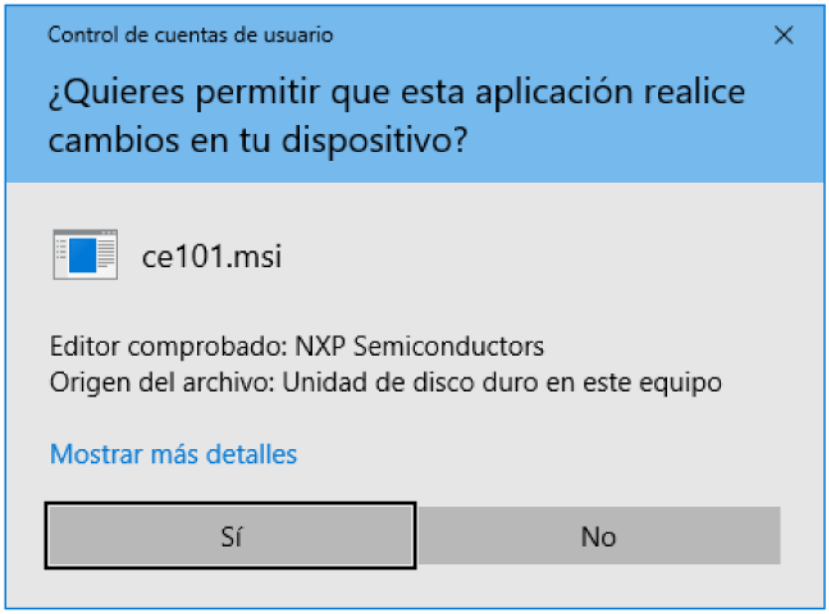
Windows le preguntará si desea desinstalar "*IDProtect CLient x.xx.xx*". Haga click en "*Sí*".



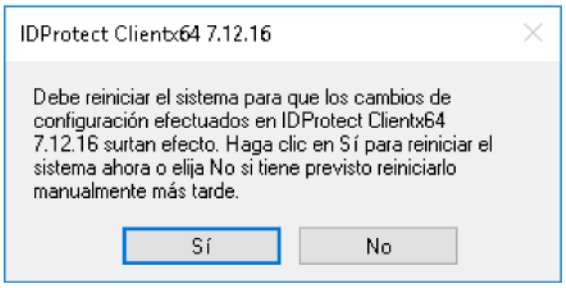
Espere mientras IDProtect Client se prepara para la desinstalación.



Se le requerirá que permita la ejecución de un paquete firmado por "*Athena Smartcard Solutions*" para realizar la desinstalación. Haga click en "*Sí*".



Espere mientras se desinstala el middleware. Al finalizar, IDProtect Cliente le informará que debe reiniciar el sistema para finalizar con la desinstalación. Haga click en "*Sí*" para reiniciar o "*No*" para reiniciar manualmente más tarde.



5 Instalación por línea de comandos

Para instalar IDProtectClient por línea de comandos refiérase a la guia "*Instalación_por_Linea_de_Comandos_MS-IDProtect*".

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:

https://www.macroseguridad.net/docs

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

- Mail: soporte@macroseguridad.net
- Portal de soporte: https://soporte.macroseguridad.la
- Web: www.macroseguridad.net