"Firma y Encripción de correo electrónico en Mozilla Thunderbird con los Tokens USB de Macroseguridad"

Nombre del Partner	Mozilla Thunderbird
Nombre de la Solución	Dispositivos Criptográficos de Macroseguridad (Tokens USB y Smartcards)
Fecha	25 de agosto de 2016

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

Revisiones:

Versión	Autor	Fecha	Comentarios
1.0	Mauro Gilardenghi	10-Dic-2011	Creación de la Guía Thunderbird
1.1	Pablo Lloveras	19-Dic-2011	Revisión y actualización.
1.2	Diego Laborero	03-Ene-2012	Aprobación final del documento
1.3	Pablo Lloveras	21-Feb-2013	Actualización
1.4	Pablo Lloveras Diego Laborero	11-Sep-2015	Actualización y Correcciones
1.5	Pablo Lloveras Guillermo Nievas	24-Ago-2016	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.org

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 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

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 6.40.03 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 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 Thunderbird**.

3 ¿Qué es Mozilla Thunderbird?

Mozilla Thunderbird es un cliente de correo electrónico, 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 Thunderbird

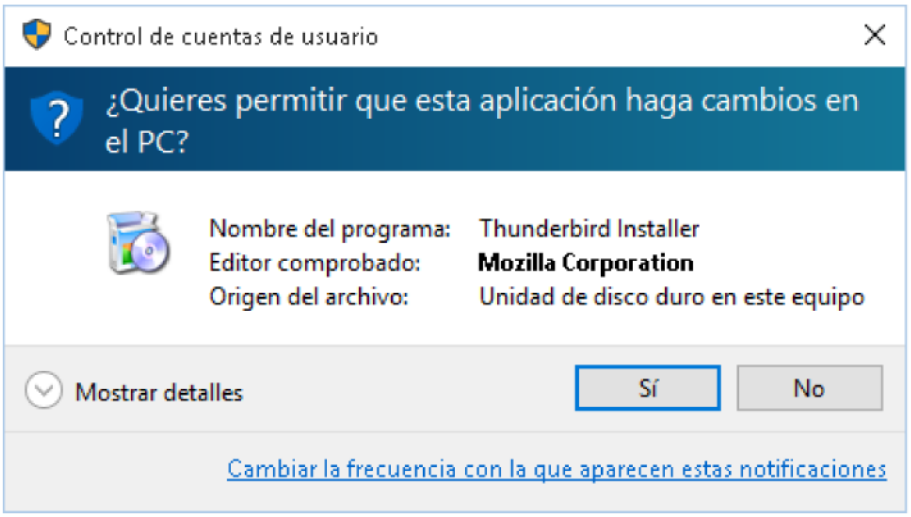
4.1 Requisitos para la instalación

- Pentium 4 o Procesadores que soporten SSE2
- 1 GB de RAM
- 200 MB de espacio en disco
- Microsoft Windows XP, Windows Vista, Windows 7, Windwos 8, Windows 10 Windows Server 2003 o superior.

4.2 Comenzar la instalación de Mozilla Thunderbird

El software es gratuito y se puede descargar de la página oficial de Mozilla https://www.mozilla.org/thunderbird/ le recomendamos que descargue la versión en castellano ya que el software es muy conocido y posee versiones en varios idiomas.

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



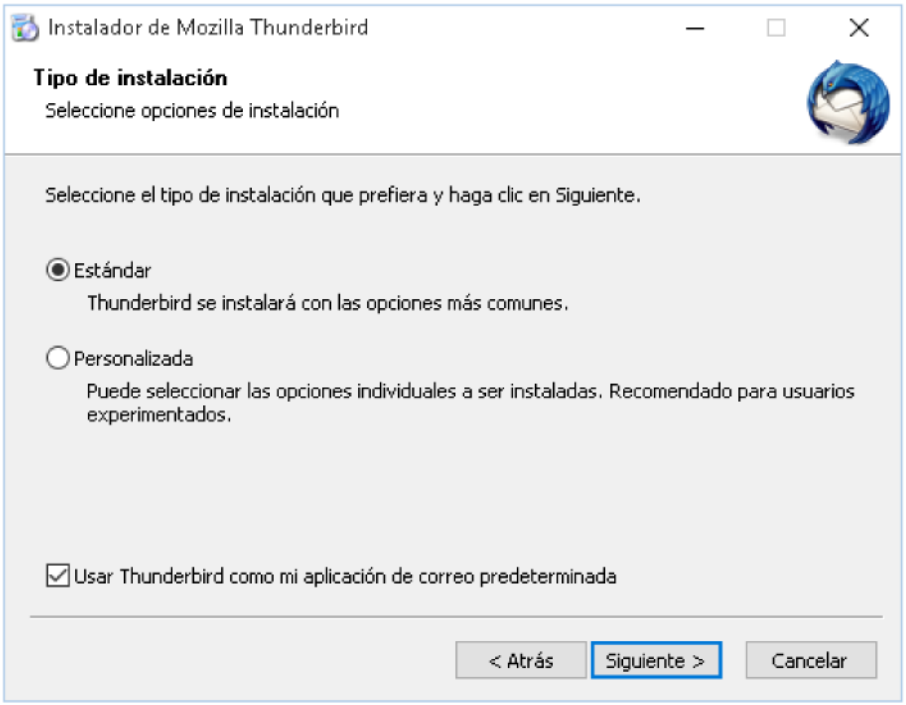
Luego se mostrará la pantalla de bienvenida del asistente, como se muestra a continuación. Haga click en "*Siguiente* >" para continuar.

Seleccione el tipo de instalación: "*Estándar*" o "*Personalizada*".

- La instalación "*Personalizada*" se recomienda sólo para usuarios experimentados, el usuario deberá elegir cuales opciones serán instaladas, especificaciones particulares como la carpeta de instalación, los íconos de acceso directo o descarga de módulos adicionales.

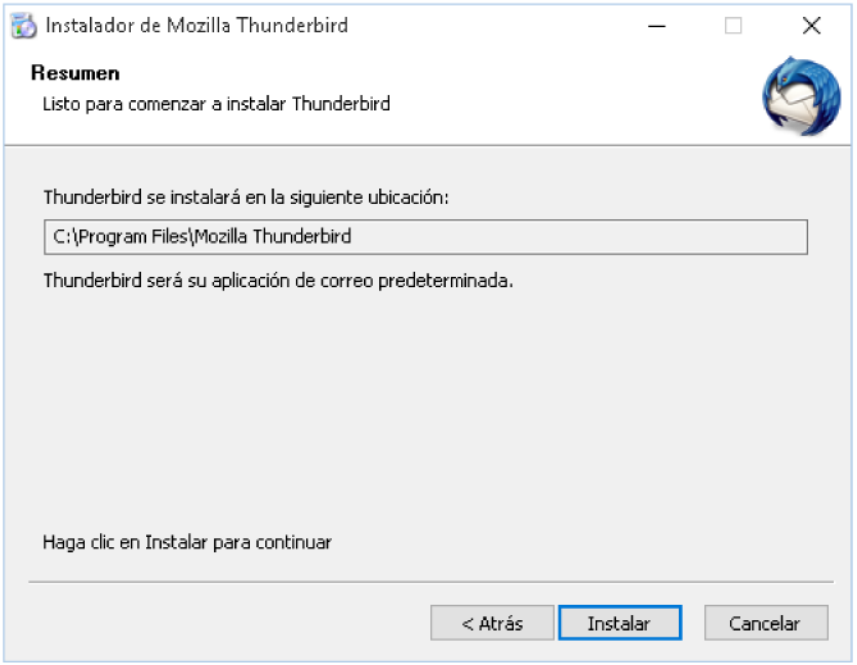
- Para el resto de los usuarios es recomendable la instalación "*Estándar*". En esta guía se utilizará este tipo de instalación.

Seleccione "*Usar Thunderbird como mi aplicación de correo predeterminada*" si desea que Mozilla Thunderbird sea su cliente de correo por defecto. Haga click en "*Siguiente* >" para continuar.

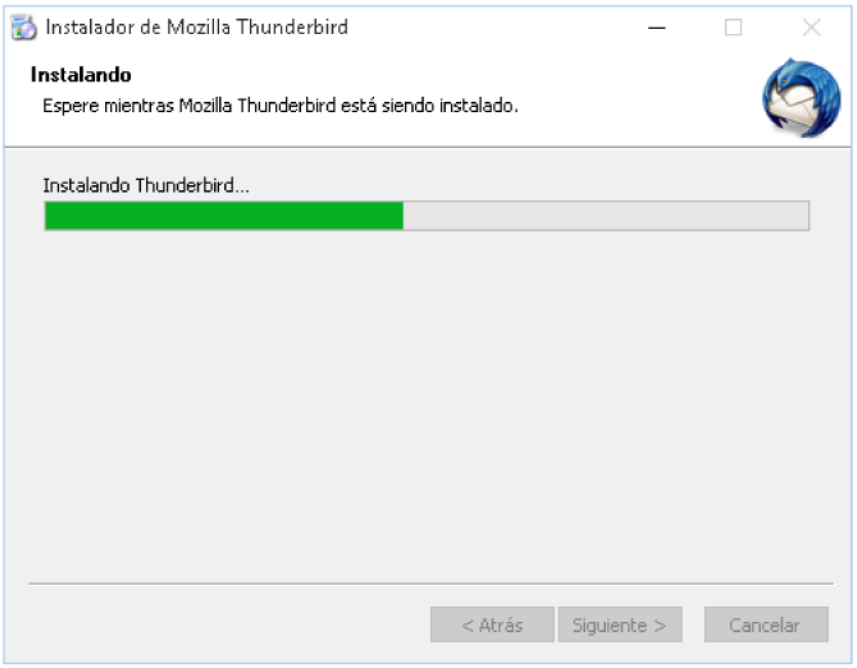


A continuación se mostrará el directorio de instalación de Mozilla Thunderbird. Como consecuencia de haber seleccionado, en el paso anterior, el tipo de instalación "*Estándar*", el directorio por defecto será el definido por el instalador.

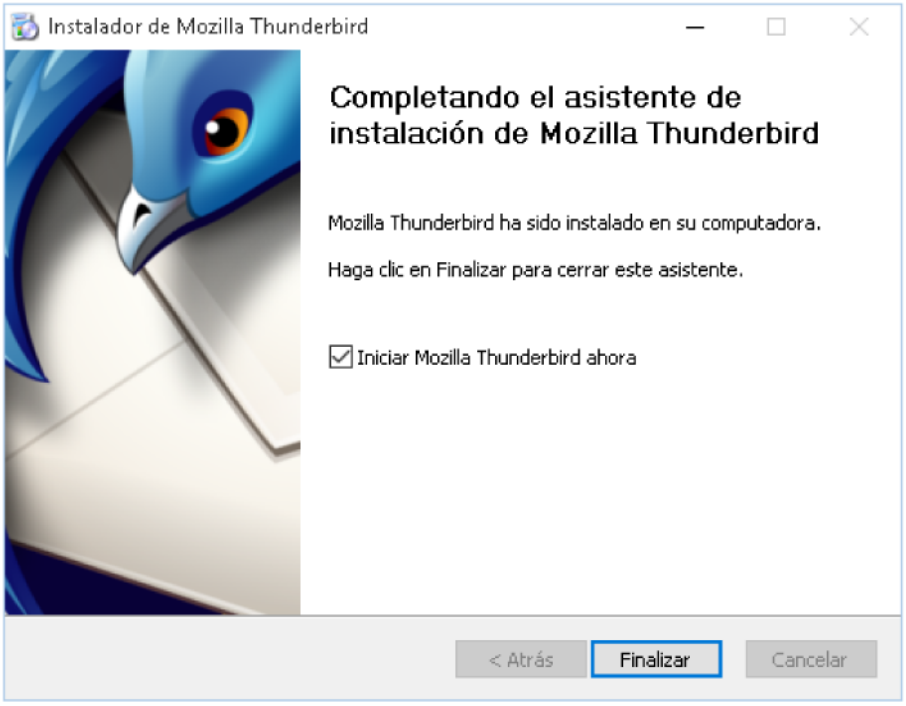
Adicionalmente informa que Mozilla Thunderbird será la aplicación de correo predeterminada ya que se indicó en el paso anterior. Haga click en "*Instalar*" para iniciar la instalación de Mozilla Thunderbird.



Espere mientras Mozilla Thunderbird se instala en su equipo.



Seleccione la opción "*Iniciar Mozilla Thunderbird ahora*" para que el programa se ejecute una vez finalizado el proceso de instalación y luego haga click en "*Finalizar*".



5 Configuración inicial de Mozilla Thunderbird

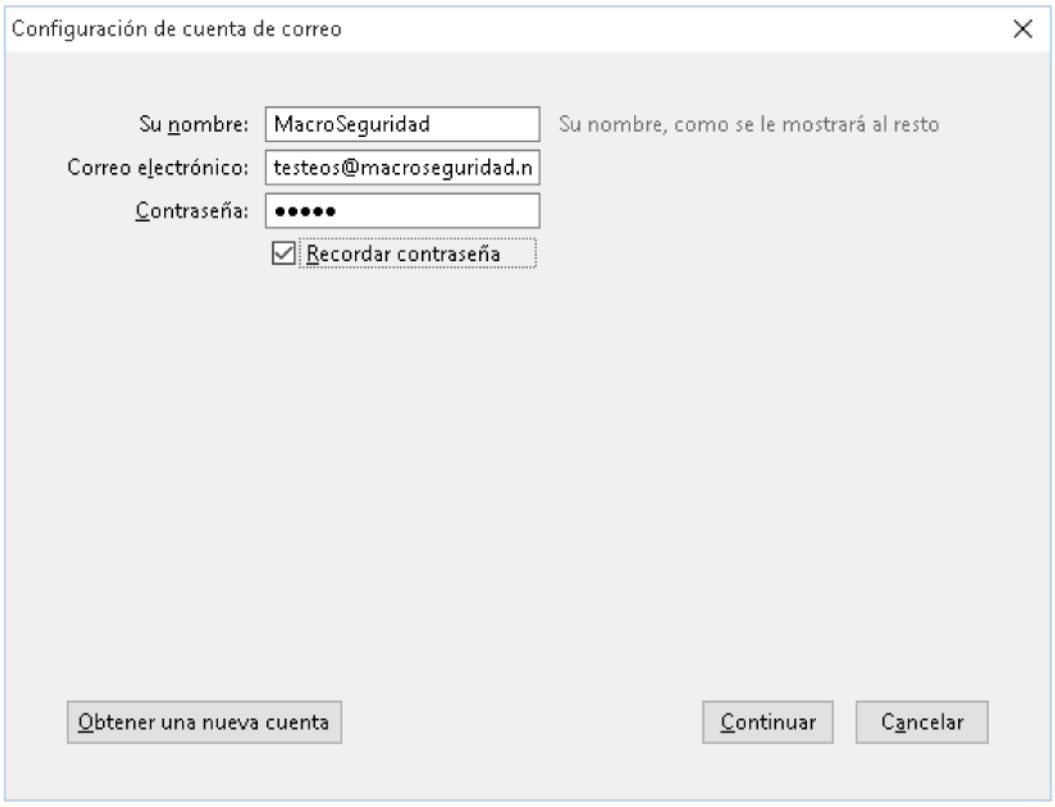
Al abrir el programa por primera vez, se iniciará el asistente de cuentas. A continuación deberá configurar una cuenta de Correo para el envío y recepción de correos electrónicos, también podrá agregar la opción de que los mismos sean firmados digitalmente y/o encriptados.

El campo "*Su nombre*" hace referencia a una breve descripción que le permitirá a los destinatarios de sus correos identificarlo.

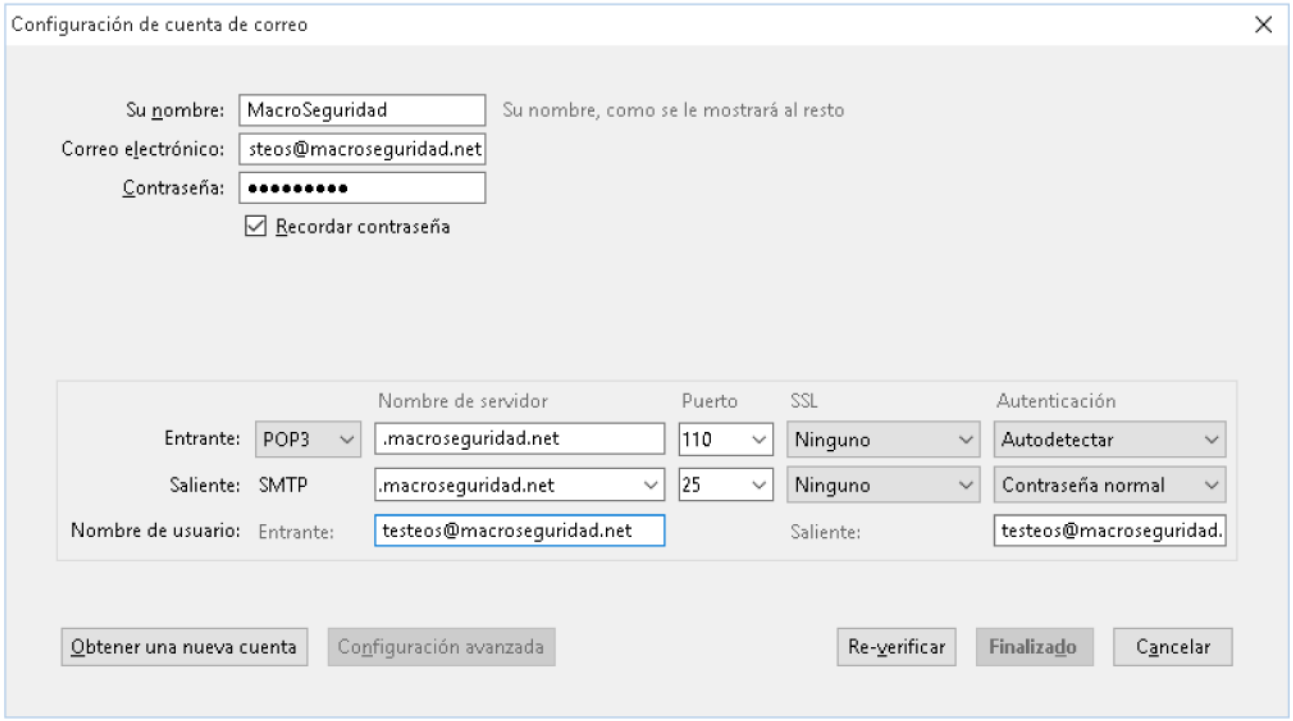
El campo "*Correo electrónico*" será la dirección de su cuenta, desde donde podrá enviar y recibir correos electrónicos.

El campo "*Contraseña*" será la password que le permitirá acceder a su cuenta.

Una vez completados los campos requeridos haga click en "*Continuar*" para proseguir con la configuración.



El asistente de configuración de cuentas de correo le solicitará que ingrese los datos del servidor de correo entrante y saliente, como se muestra a continuación:



Puede optar por dos tipos de conexión diferentes: POP o IMAP. Consulte con su administrador de sistemas o con el proveedor del servicio acerca del tipo de conexión entrante del servidor de correo. Una vez que haya seleccionado el tipo de conexión, deberá ingresar el nombre del servidor. Finalmente, se le pedirá que especifique el servidor de correo saliente de su cuenta.

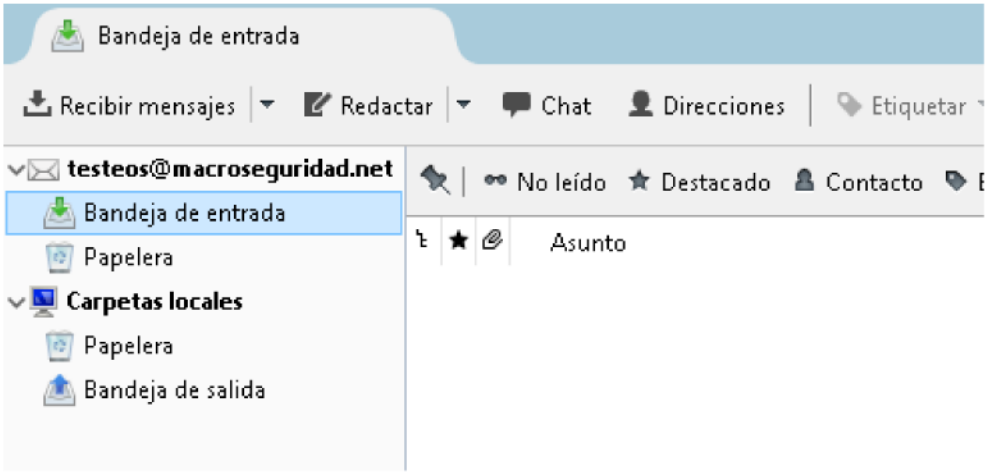
Nota: En el punto 6 “Configurar librería PKCS#11 de los Token USB y SmartCards de Macroseguridad.org en Mozilla Thunderbird” se explican los pasos necesarios para integrar los dispositivos criptográficos con esta aplicación.

En resumen, la información que necesitará conocer al momento de configurar una cuenta de correo es la siguiente:

- Tipo de servidor entrante: POP o IMAP
- Nombre del servidor entrante y su puerto correspondiente
- Nombre del servidor saliente y su puerto correspondiente

En caso de no conocer alguno de estos datos, solicítelo al proveedor del servicio o al administrador de la institución o de la empresa para terminar con la configuración de su cuenta de correo. Haga click en "*Crear cuenta*" para finalizar con el asistente de configuración de cuentas de correo.

Se mostrará la ventana principal de Mozilla Thunderbird. Esto indica que ha finalizado con la configuración correctamente por lo que el software ya se encuentra en condiciones de enviar y recibir mails.



5.1 Recibir Mails

Para recibir los mails de cada una de las cuentas de correo, previamente configuradas, de forma simultánea haga click sobre la barra de herramientas en "*Recibir Mensajes*" (figura 1). Si, en cambio, su intención es recibir sólo aquellos mails pertenecientes a una cuenta en particular haga click sobre la flecha que se encuentra a la derecha de "*Recibir Mensajes*", se desplegará un menú como el de la figura 2, y luego sobre el nombre de la dirección de correo electrónico que desee.

Note que en el menú desplegado anteriormente se lista sólo la cuenta de correo que ha sido configurada previamente (figura 2).

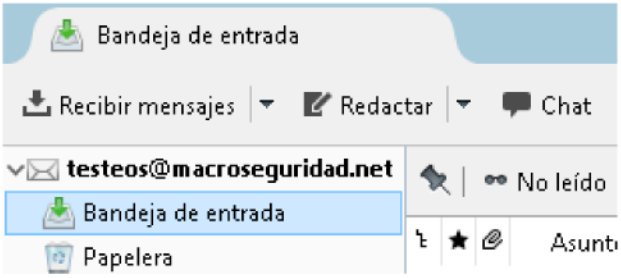


Figura 1

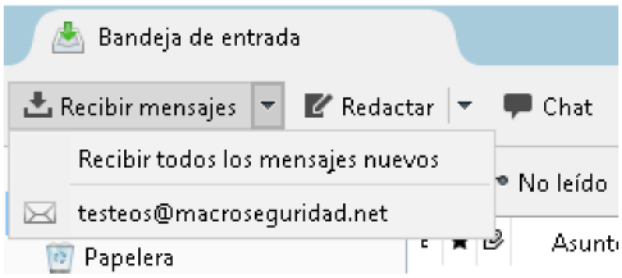
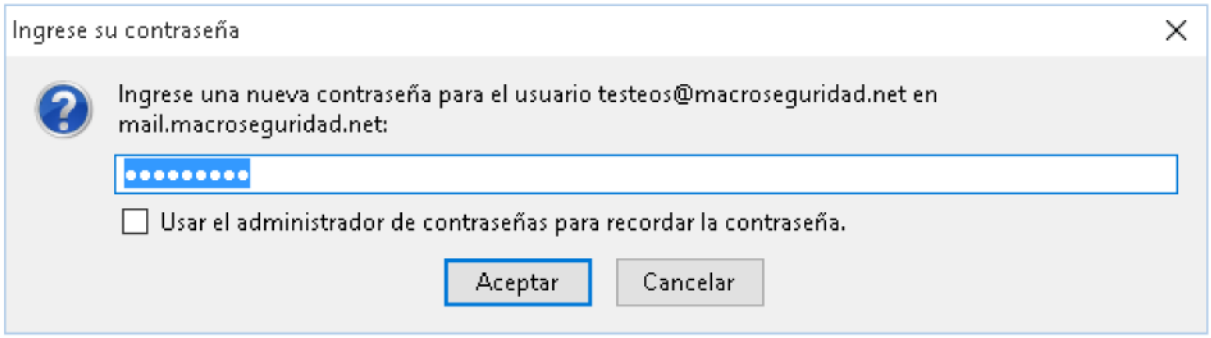


Figura 2

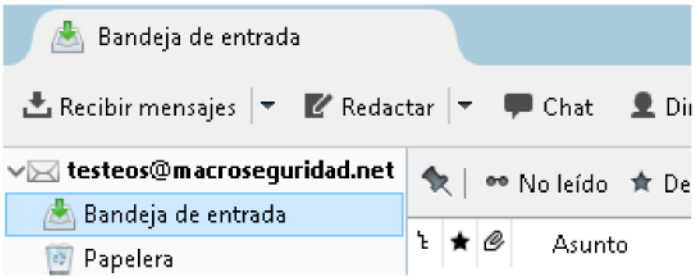
Ya sea haciendo click sobre "*Recibir Mensajes*" o seleccionando su cuenta desde el menú, el programa le preguntará por la password de su cuenta para conectarse con el servidor (en caso que no la haya guardado cuando configuró su cuenta).



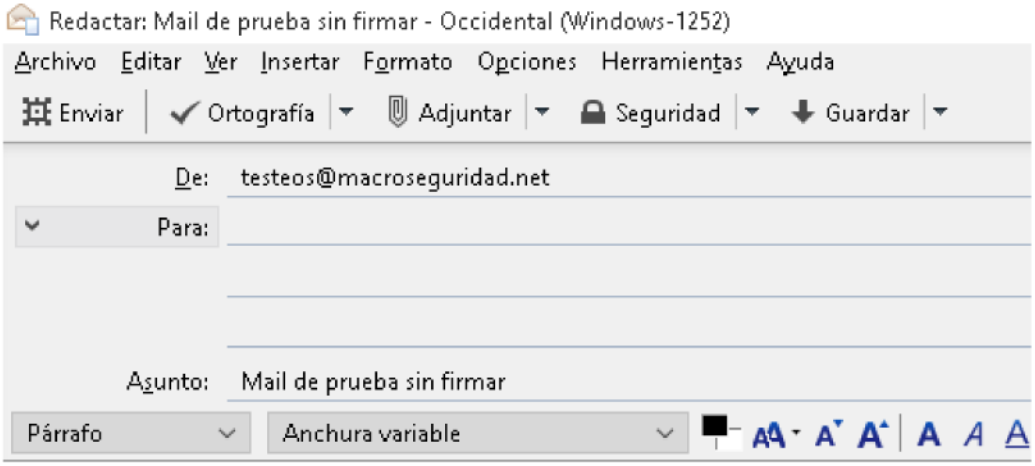
Si selecciona la opción "*Usar el administrador de contraseñas para recordar la contraseña*" el programa recordará la contraseña ingresada para esta cuenta. Haga click en "*Aceptar*" para comenzar con el proceso de recuperación de mensajes desde el servidor.

5.2 Redactar un mail

Para redactar un mail debe hacer click, sobre la barra de herramientas del programa, en "*Redactar*".



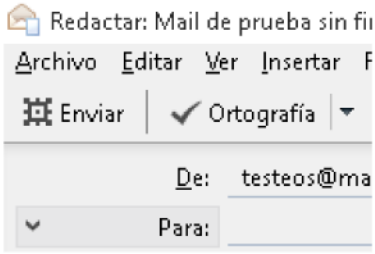
Se abrirá una nueva ventana con las herramientas de redacción de correo, como se muestra a continuación. Los campos que usted debe completar son: "*De*", "*Para*", "*Asunto*" además de escribir el contenido del correo.



Es un mail de prueba sin encriptar ni firmar.

En el campo del remitente se mostrará la cuenta de correo configurada por defecto.

Una vez completados los campos requeridos, simplemente haga click en el botón "*Enviar*", que se encuentra en la barra de herramientas de la ventana de redacción de correo, y su correo será enviado.



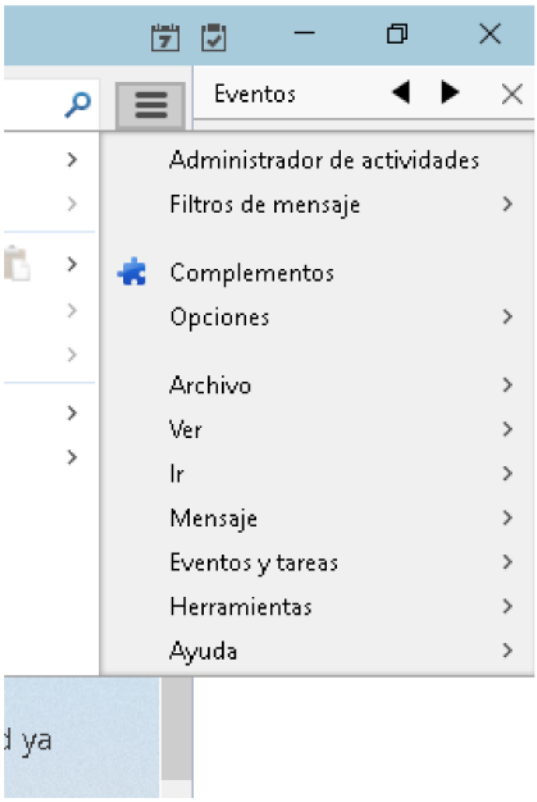
6 Configurar librería PKCS#11 de los Token USB y SmartCards de Macroseguridad.org en Mozilla Thunderbird

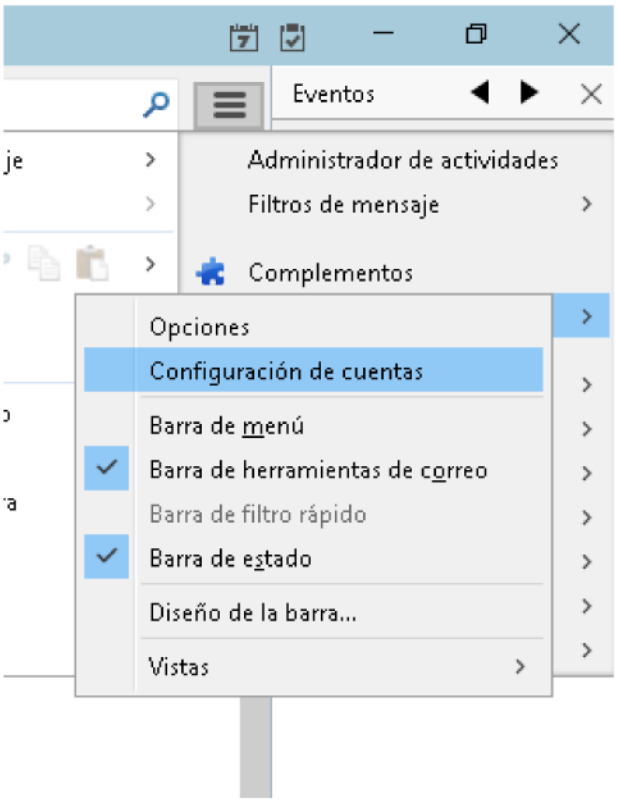
6.1 Configurar los Token USB/Smartcard MS-IDProtect

Antes de enviar mails firmados o encriptados utilizando un Token USB / SmartCard de Macroseguridad deberá configurar el Mozilla Thunderbird para que pueda interactuar con el dispositivo criptográfico.

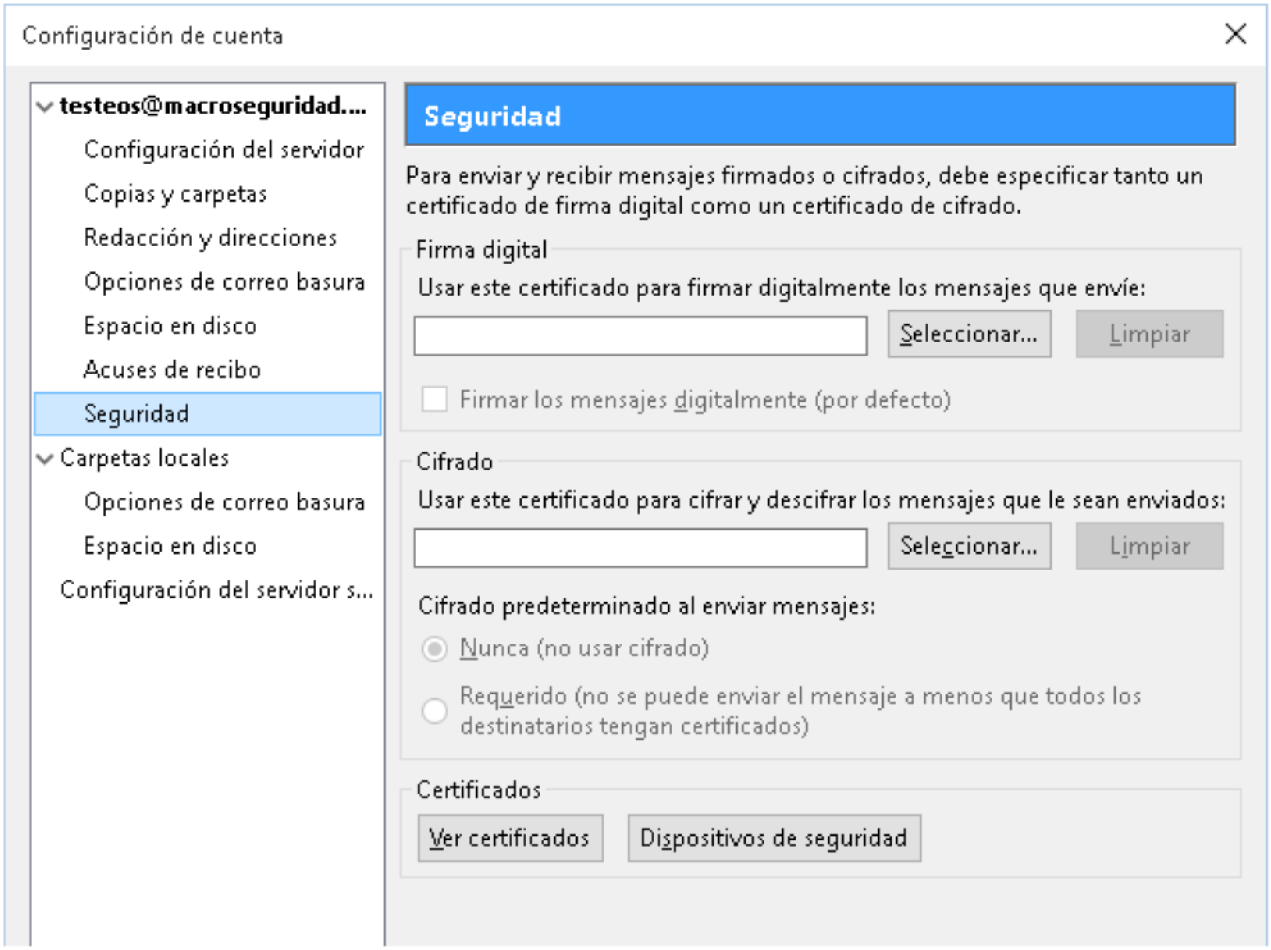
Esta clase de aplicaciones (como por ejemplo Thunderbird, Firefox, OpenVPN, PGP, etc.) trabajan con dispositivos criptográficos (smartcards, Tokens USB, etc.) a través de uno de los estándares más conocidos del mercado denominado PKCS#11.

Haga click en el botón de menú,luego en "*Opciones*" y finalmente en"*Configuración de cuentas*".

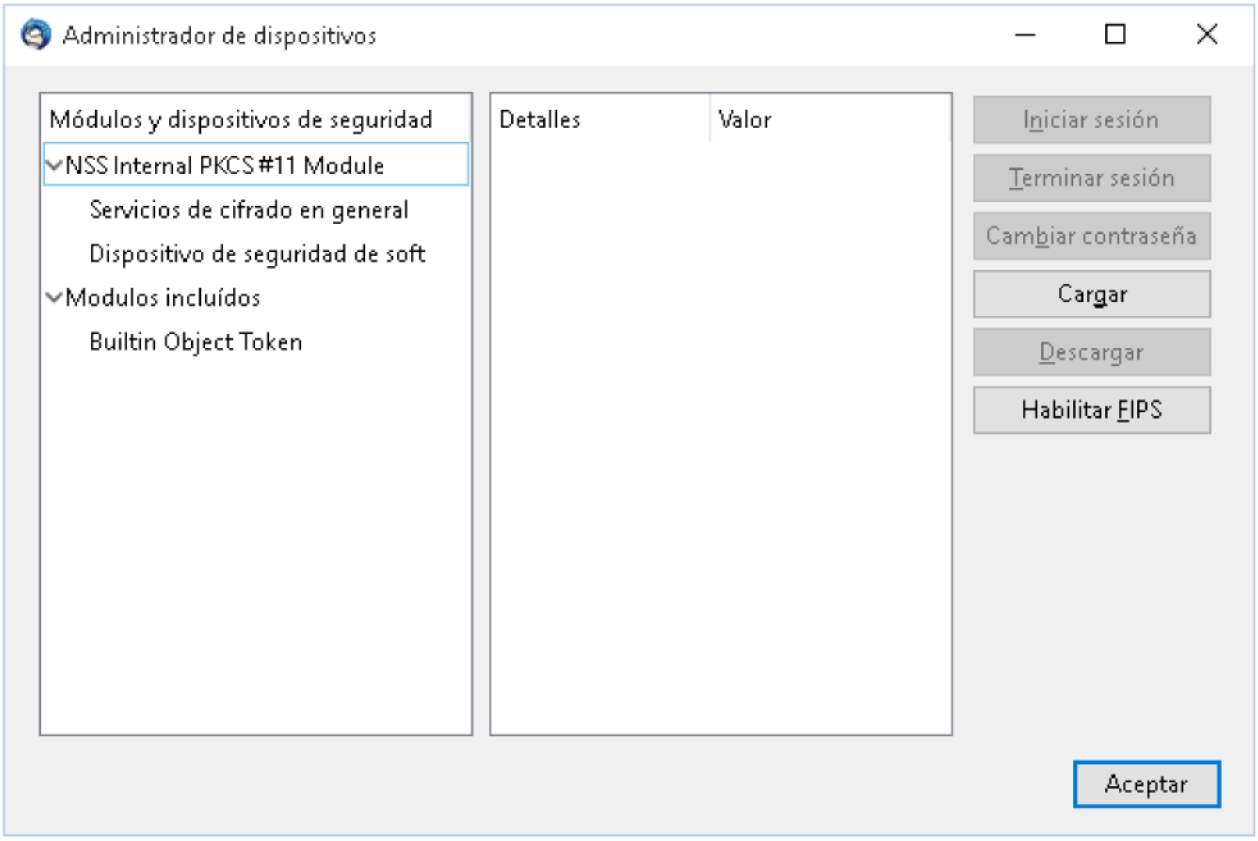




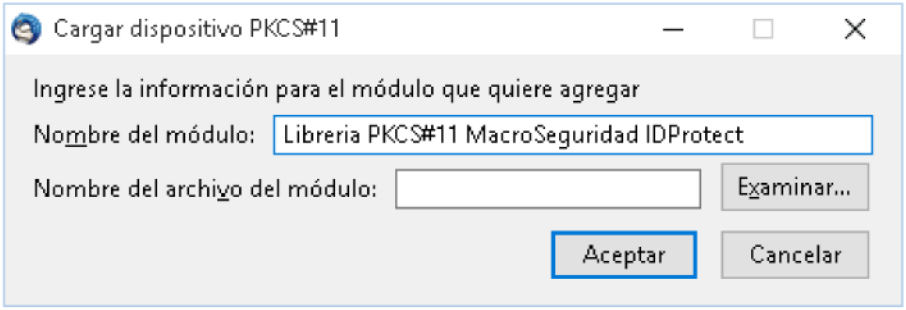
A continuación se mostrará la siguiente ventana. En el panel izquierdo de esta ventana, donde están listadas las cuentas de correo, seleccione su cuenta para expandir las opciones. Haga click en "*Seguridad*". En el panel derecho de la ventana encontrará la sección "*Certificados*". Dentro de la misma, haga click en "*Dispositivos de seguridad*".



Se mostrará la ventana "*Administrador de dispositivos*". Sobre el margen superior derecho de la ventana, haga click en "*Cargar*". Esto le permitirá adicionar el módulo PKCS#11 de MacroSeguridad para poder interactuar con los dispositivos criptográficos MS-IDProtect.



A continuación se mostrará la siguiente ventana:



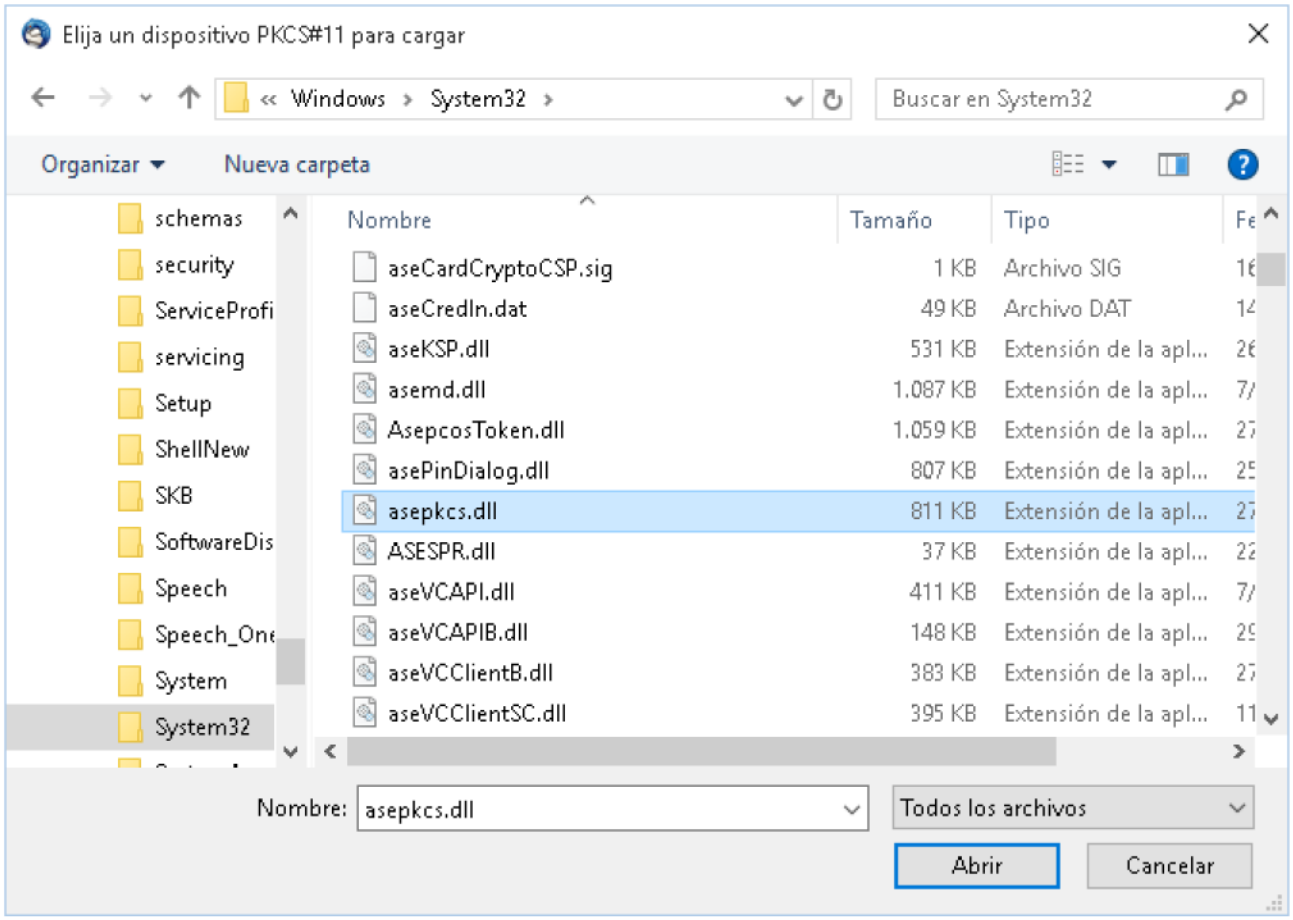
Ingrese el nombre del módulo PKCS#11 del dispositivo que desea agregar. A modo de ejemplo se utiliza "*Libreria PKCS#11 MacroSeguridad IDProtect*". Se recomienda ingresar un nombre referido al producto en cuestión.

Luego, haga click en "*Examinar*" para buscar y seleccionar la librería PKCS#11 que le permitirá a Mozilla Thunderbird interactuar con el dispositivo.

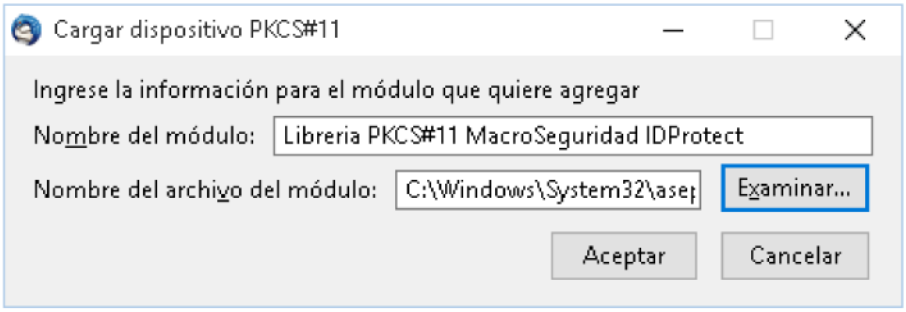
Nota: Si Ud. está utilizando Mozilla Firefox o Thunderbird, le sugerimos no utilizar palabras que requieran tilde, debido a que generan conflictos cuando se intenta eliminar el módulo cargado. Es un problema ya reportado a Mozilla.

La librería que refiere al módulo PKCS#11, que se crea al momento de la instalación del middleware del MS-IDProtect, se llama "*asepkcs.dll*", la misma se encuentra en "*C:\Windows\system32*" siendo "*C*" la unidad donde instaló su Sistema Operativo.

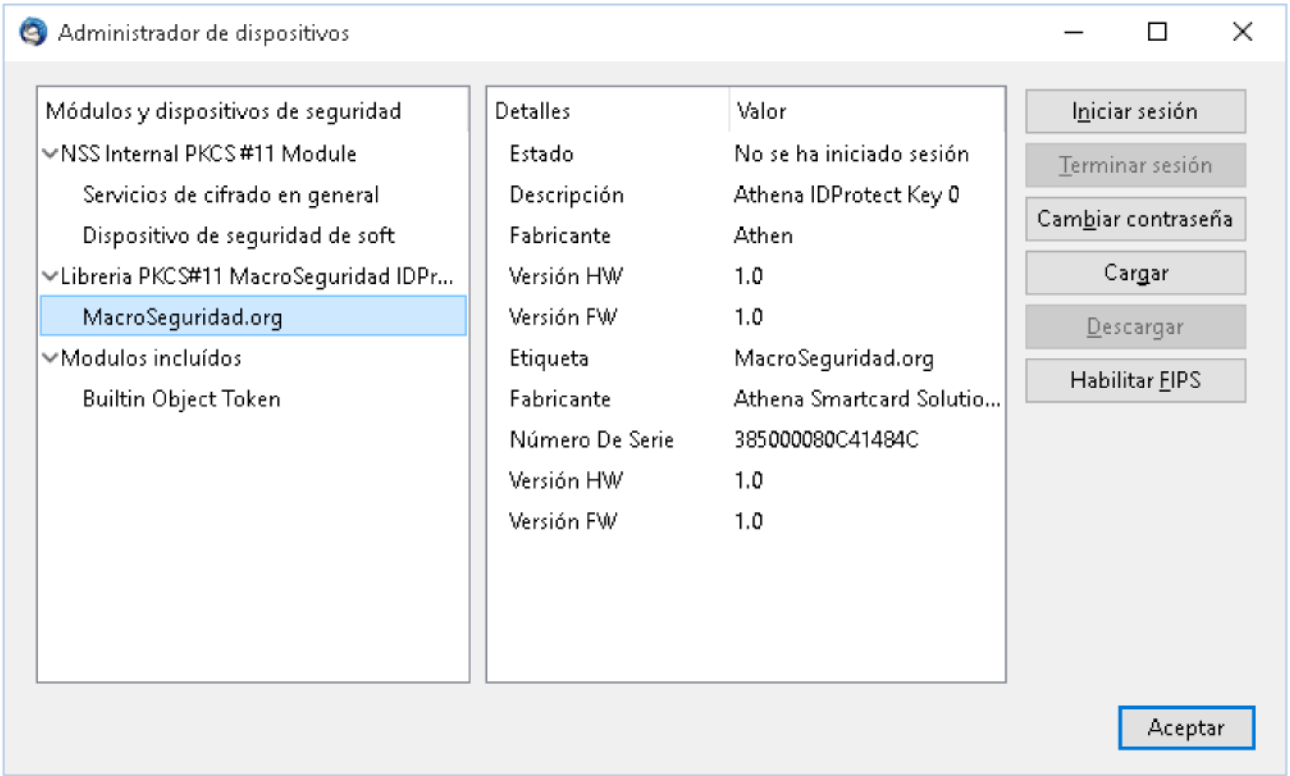
Una vez seleccionada la librería haga click en "*Abrir*". De no encontrarlo, es posible que se deba a que el middleware no fue instalado correctamente. Verifique que los mismos hayan sido instalados correctamente.



Haga click en "*Aceptar*" para finalizar con la adición del módulo.



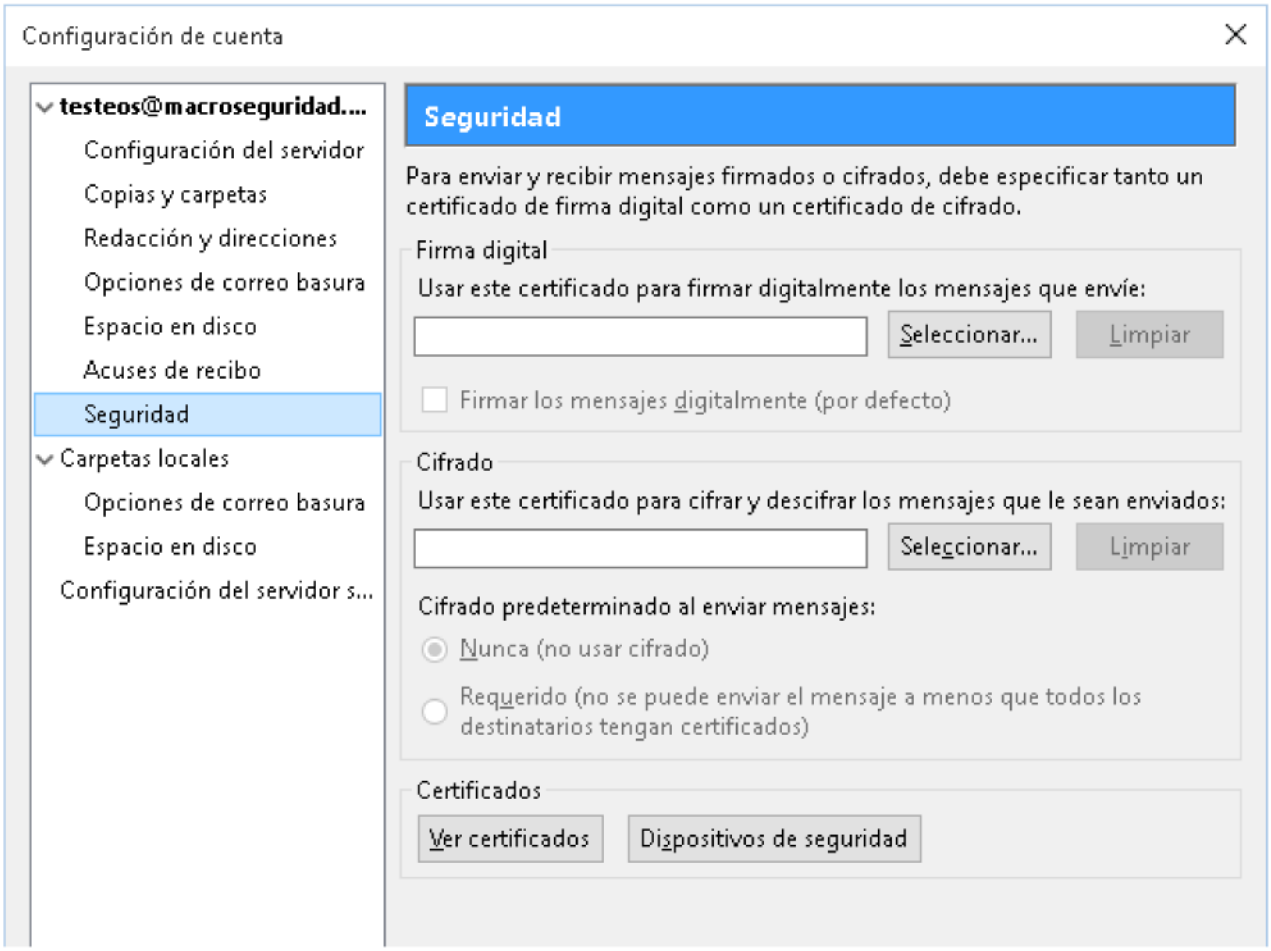
Volverá a la ventana del administrador de dispositivos, donde podrá verificar los Tokens USB / Smartcards que se encuentran presentes así como también información referida a ellos, como se muestra a continuación. Haga click en "*Aceptar*" para cerrar el Administrador de dispositivos.



6.2 Seleccionar un certificado almacenado dentro de un MS-IDProtect

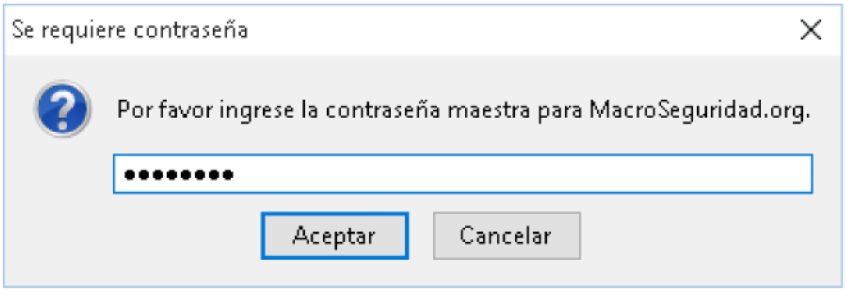
En la ventana "Configuración de cuentas" haga click sobre "*Seguridad*".

Sobre el margen superior derecho, bajo la sección de "Firma Digital", haga click en "*Seleccionar…*".

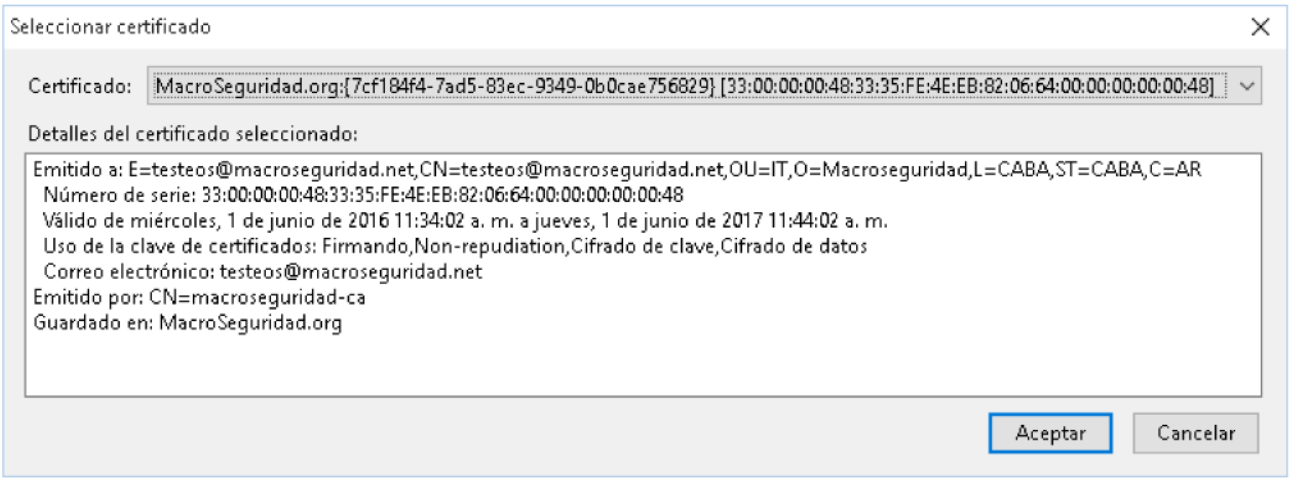


El programa buscará todos los certificados que se encuentren tanto en el repositorio de Mozilla Thunderbird como en los dispositivos MS-IDProtect conectados a la PC.

Es necesario que el Token USB / SmartCard de Macroseguridad.org se encuentre conectado antes de iniciar el Mozilla Thunderbird con algún certificado asociado a la cuenta de correo. El programa le pedirá entonces el PIN de su Token USB/SmartCard para poder acceder al contenido del mismo.

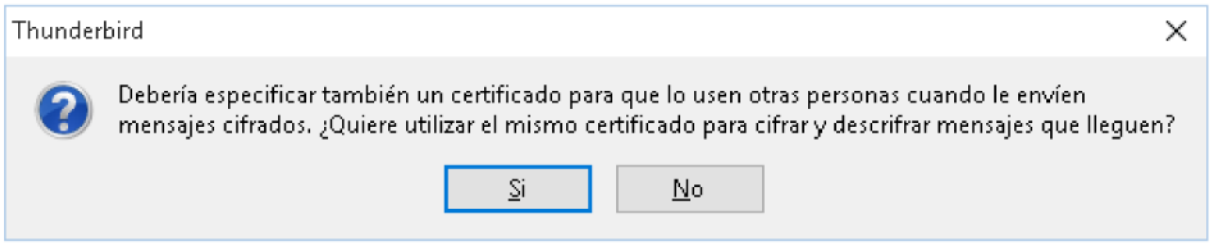


Si no posee ningún certificado dentro de su MS-IDProtect, ni en el repositorio de Thunderbird, se mostrará una ventana advirtiendo que no se ha encontrado ningún certificado. Caso contrario, se mostrará una ventana como la siguiente. Seleccione de la lista el certificado que desea utilizar para firmar digitalmente los mails, y haga click en "*Aceptar*".

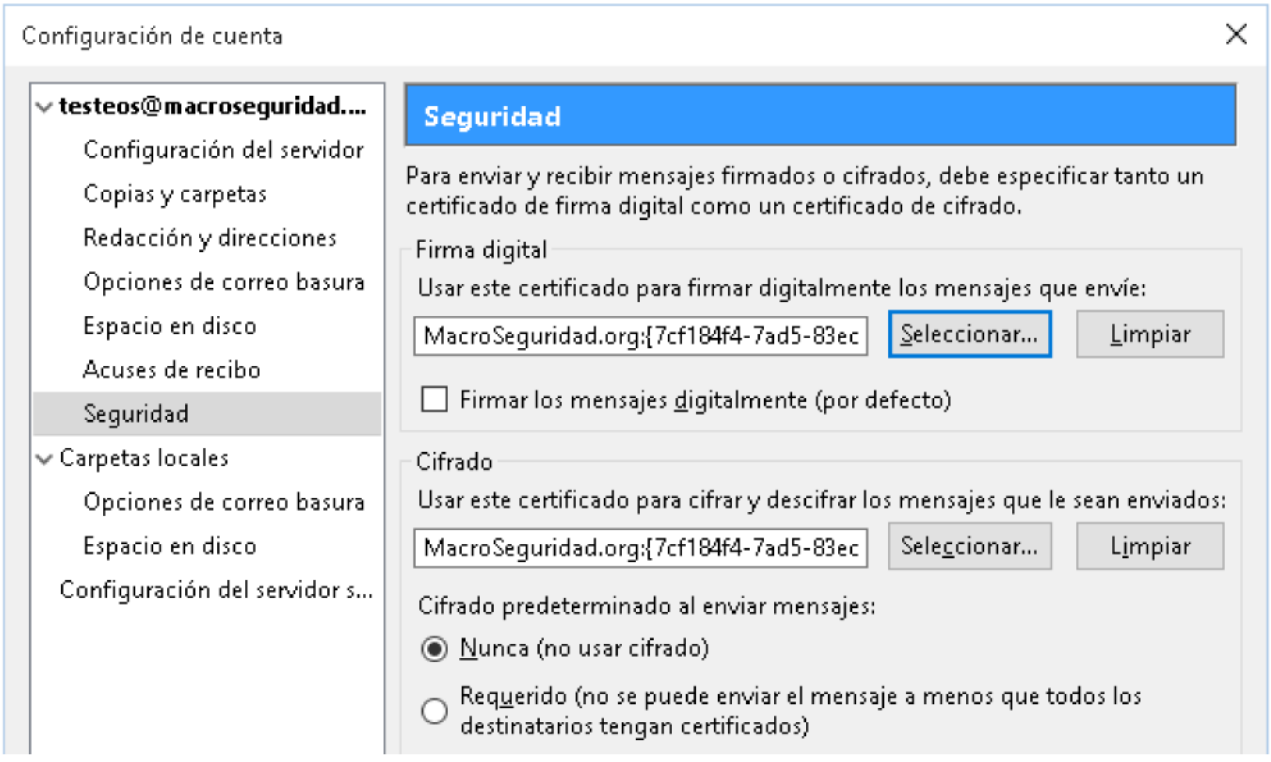


Los certificados que estén almacenados en el dispositivo MS-IDProtect empezarán con el nombre del dispositivo seguido por el nombre del certificado. Los certificados almacenados en Thunderbird, no tendrán prefijo. Por ejemplo, en la imagen anterior, existe un certificado para testeos@macroseguridad.net dentro del dispositivo llamado

IDProtect. Seleccione el certificado que se encuentra almacenado en el MS-IDProtect. El programa le preguntará si desea utilizar el mismo certificado para encriptar y desencriptar mails. Haga click en "*Si*" en caso afirmativo, o en "*No*" en caso contrario.



La cuenta de correo se encuentra ahora configurada tanto para firmar como para encriptar mails. En este caso, el certificado emitido por la CA Interna de Macroseguridad a las personas físicas puede ser utilizado tanto para Firma de correo como para cifrado. Por tal motivo, se estableció el mismo certificado para encripción de mails, como se muestra en la siguiente ventana. Haga click en "*Aceptar*" para concluir con la configuración de Mozilla Thunderbird con su token/smartcard MS-IDProtect.

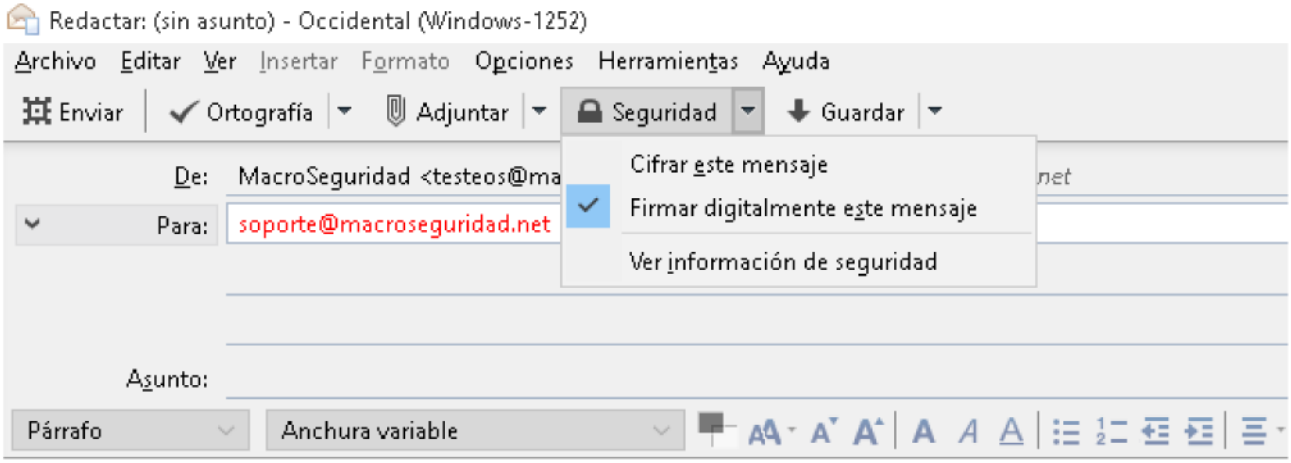


7 Utilizar un certificado almacenado dentro de su MS-IDProtect para firmar Mails

Para enviar un mail firmado digitalmente previamente debe configurar el certificado que se encuentra almacenado dentro de su MS-IDProtect (refiérase al capítulo 6.2).

Haga click en "*Redactar*", complete todos los campos necesarios del nuevo mensaje y redacte el contenido del mail.

Para firmar el correo, diríjase a la barra de herramientas y haga click en "*Seguridad*". Se desplegará un menú en el cual deberá seleccionar "*Firmar digitalmente este mensaje*". Una vez seleccionada esta opción envíe su email haciendo click en "*Enviar*".



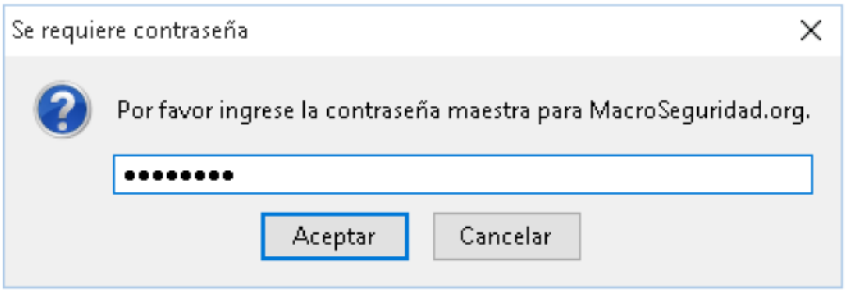
7.1 Autenticación al Token USB / SmartCard MS-IDProtect

Al hacer click en "*Enviar*" el sistema buscará el certificado previamente seleccionado para firmar el contenido del mensaje. Este certificado se encuentra almacenado dentro de su MS-IDProtect de manera segura.

Para acceder, deberá autenticarse ingresando el PIN de usuario. Es decir, se requiere un doble factor de autenticación: algo que Ud. tiene (el Token USB / SmartCard de MacroSeguridad) y algo que Ud. sabe (el PIN/Password para acceder al mismo).

El sistema le pedirá entonces que ingrese su PIN, como se muestra en la siguiente imagen. El PIN por defecto del MS-IDProtect es 12345678.

Consulte a su Administrador de la Red para mayor información o refiérase a la documentación correspondiente.



Haga click en "*Aceptar*". Si el PIN ingresado es correcto, Thunderbird podrá acceder al Token USB / SmartCard MS-IDProtect y utilizar el certificado almacenado para firmar digitalmente el correo electrónico.

Esta operación es completamente transparente. Una vez firmado, el mail será enviado junto a su firma digital.

7.2 Recibir un Mail Firmado

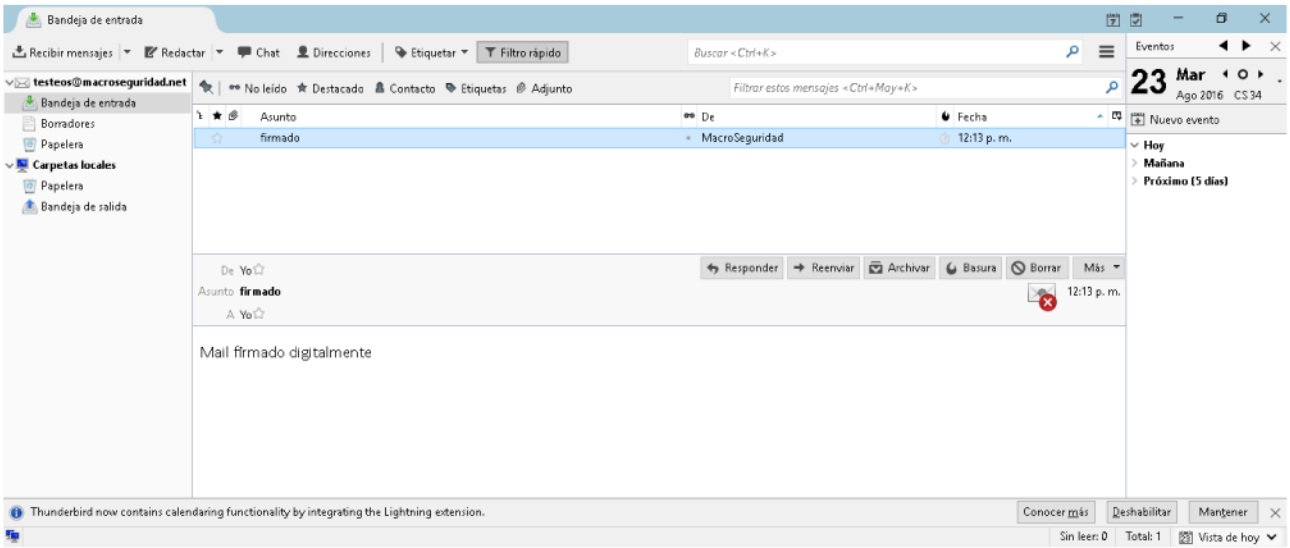
Al momento de recibir un mail firmado digitalmente pueden suceder dos cosas:

- Que el certificado con el cual se firmó el mensaje haya sido otorgado por una Autoridad Certificante (CA) de confianza (WebTrust) como es COMODO, es decir, que la clave pública de la CA ya se encuentre instalada en el repositorio de Mozilla Thunderbird.

- Que el certificado haya sido otorgado por una CA en la que no confía y debamos realizar un procedimiento particular.

Para más información sobre CAs ver Apéndice 1

En la siguiente figura se muestra lo que sucede cuando se recibe un mail firmado de una CA que no es de confianza, note que aparece un nuevo ícono indicando que no se confía.

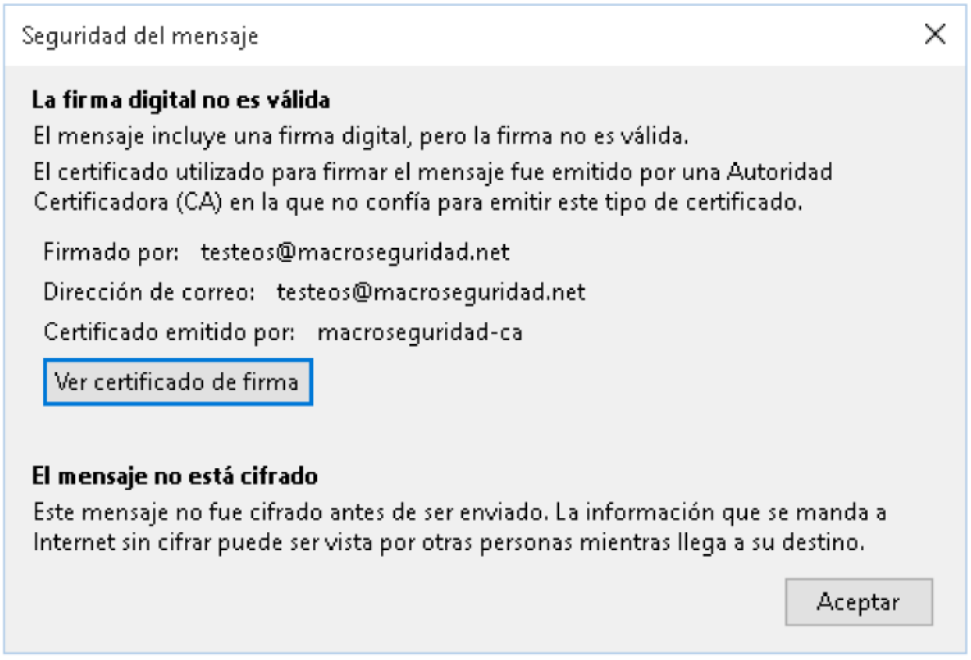


En este caso el símbolo de firma digital posee una cruz, lo que significa que la firma digital no se reconoce como válida por algún motivo.

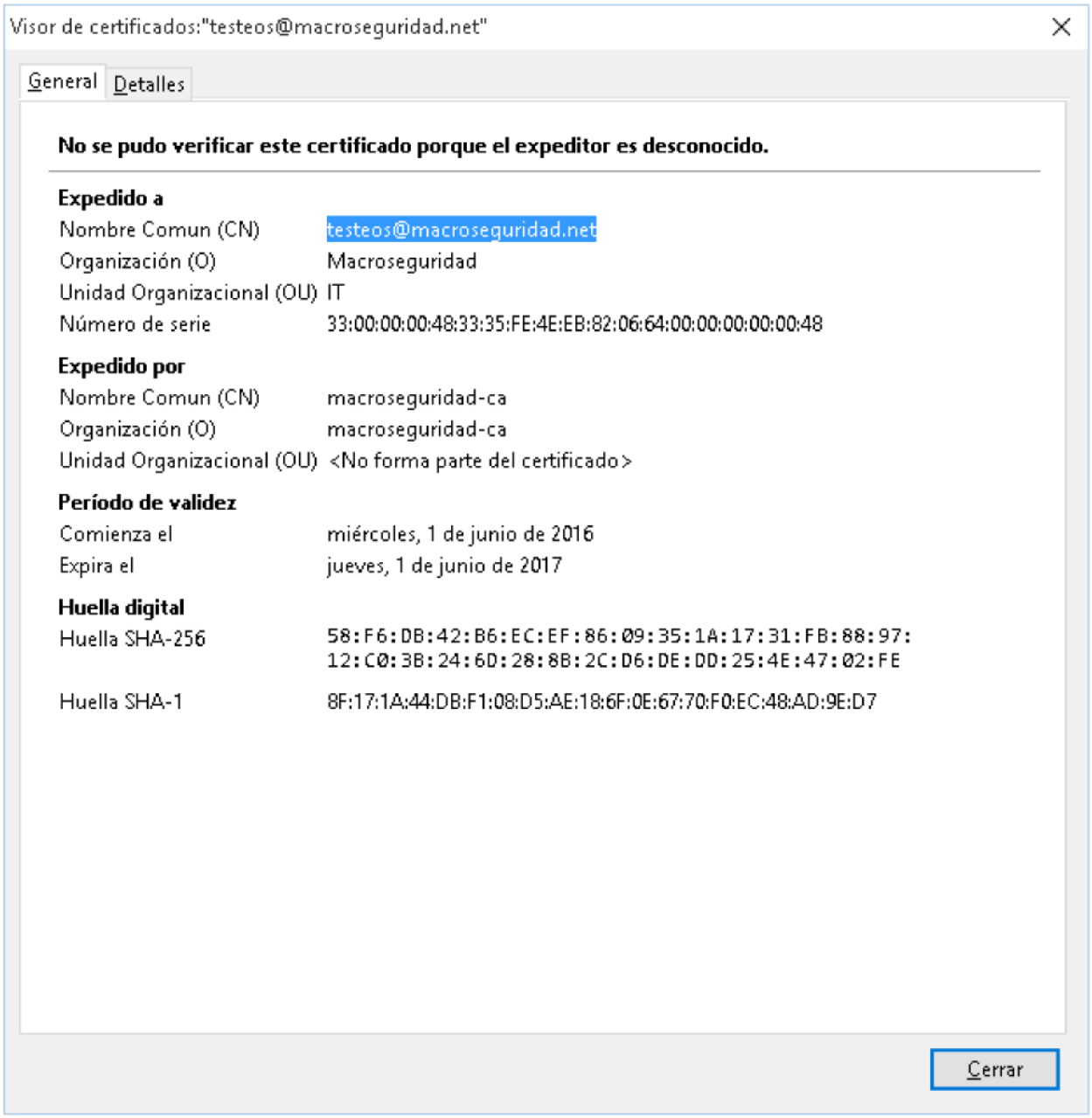
Estos motivos pueden ser diversos:

- que no se confíe en la Entidad Certificante que emitió ese certificado
- que el certificado con el cual se firmó el correo haya expirado
- que el certificado haya sido revocado

En este caso particular, el certificado es de una CA la cual NO ha sido establecida aún como una CA de confianza. Si hace click sobre este icono, aparecerá una ventana de advertencia como la que se muestra a continuación.



Este mensaje informa que la firma no es válida porque proviene de una CA que no tiene establecida la ruta de confianza. Si hace click sobre “Ver certificado de firma” podrá ver una ventana que muestra todos los detalles del certificado como se muestra a continuación.



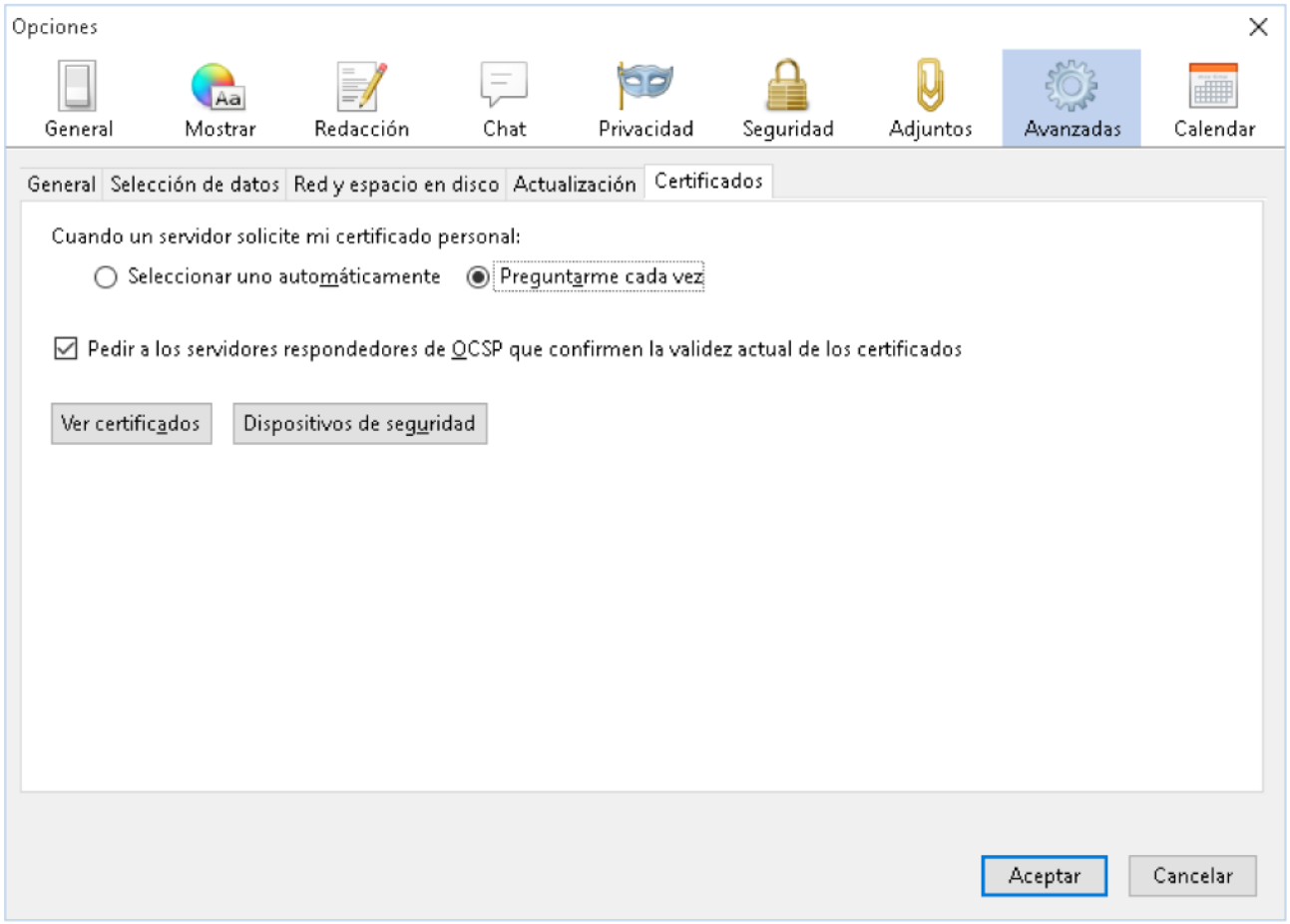
7.3 Establecer una CA como autoridad certificante raíz de confianza

A continuación se mostrará el procedimiento a seguir para establecer una CA (Certificate Authority) como una autoridad certificante de confianza. Para poder llevar a cabo esto deberá contar con el Certificado Raíz de la Autoridad Certificadora.

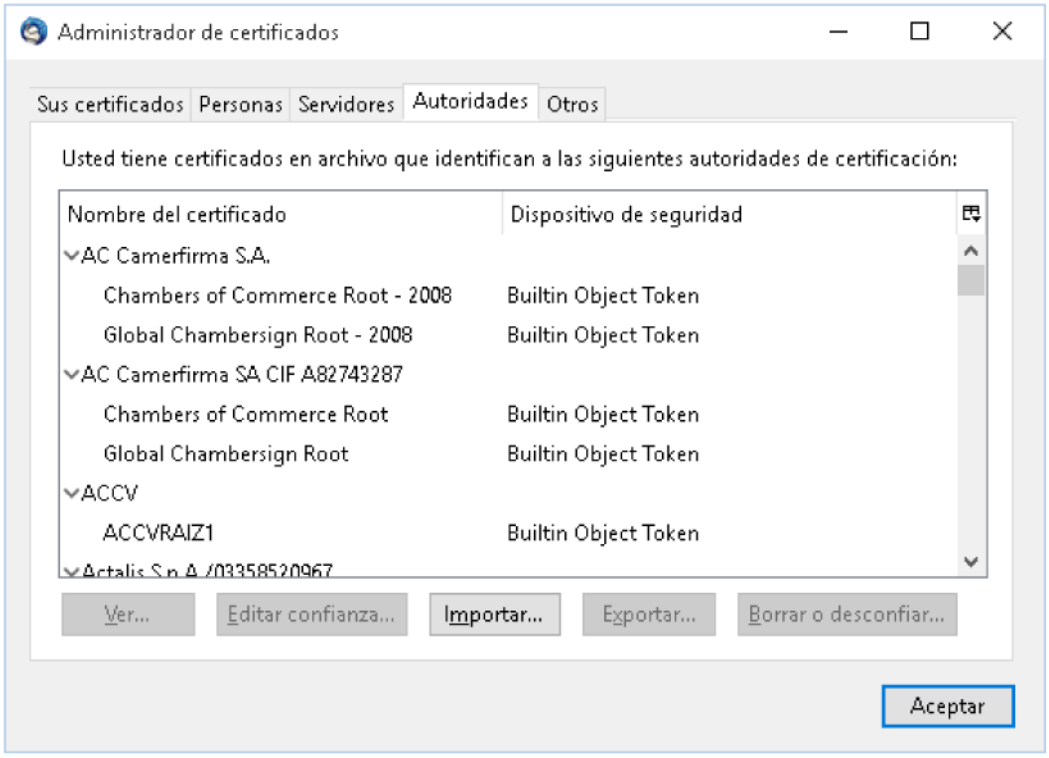
Para obtener el Certificado Raíz deberá contactarse con la CA (probablemente pueda descargar la clave pública de la CA a través de su sitio web) o solicitarle al emisor del correo electrónico firmado que se la proporcione.

Cuando ud. posea en su poder el certificado con la llave publica de la CA. Haga click en el botón de menú,luego en "*Opciones*" y finalmente en"*Opciones*".

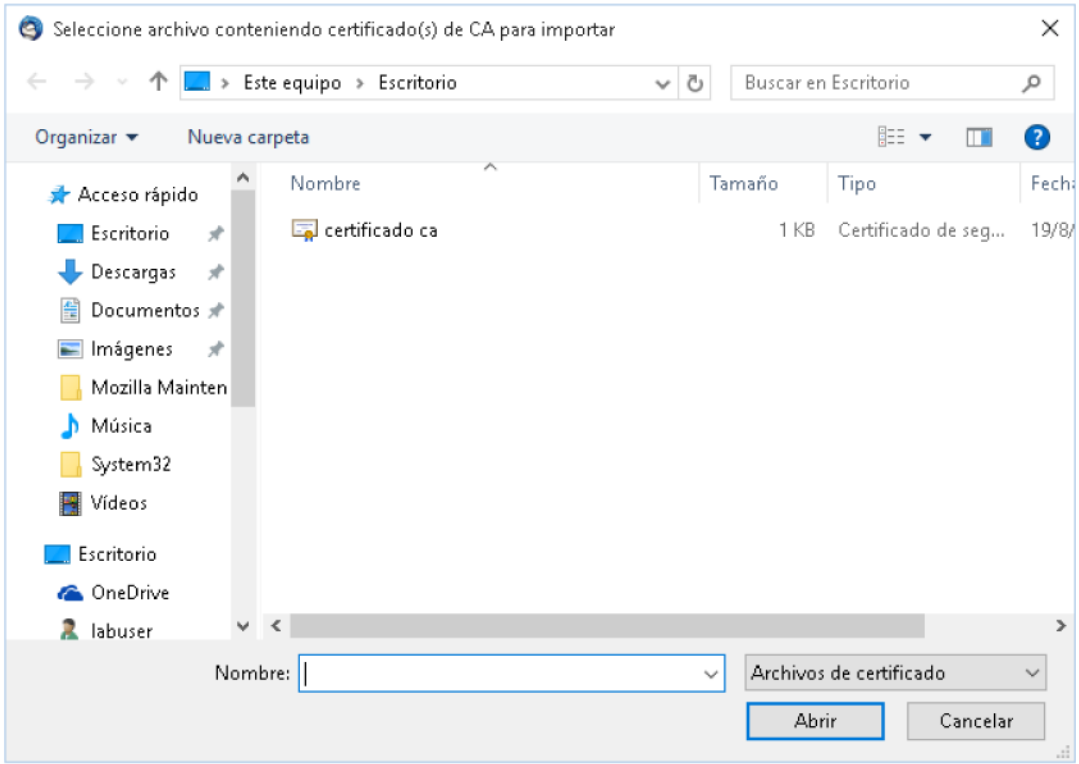
Después haga click en "*Avanzadas*", luego en la pestaña "*Certificados*" y finalmente en "*Ver certificados*" para abrir el Administrador de Certificados.



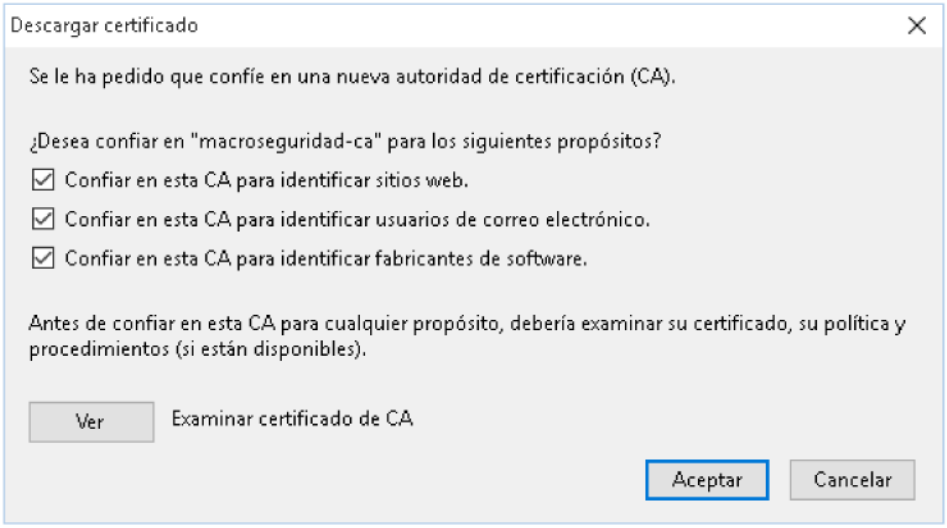
Seleccione "*Autoridades*" y luego haga click en "*Importar…*".



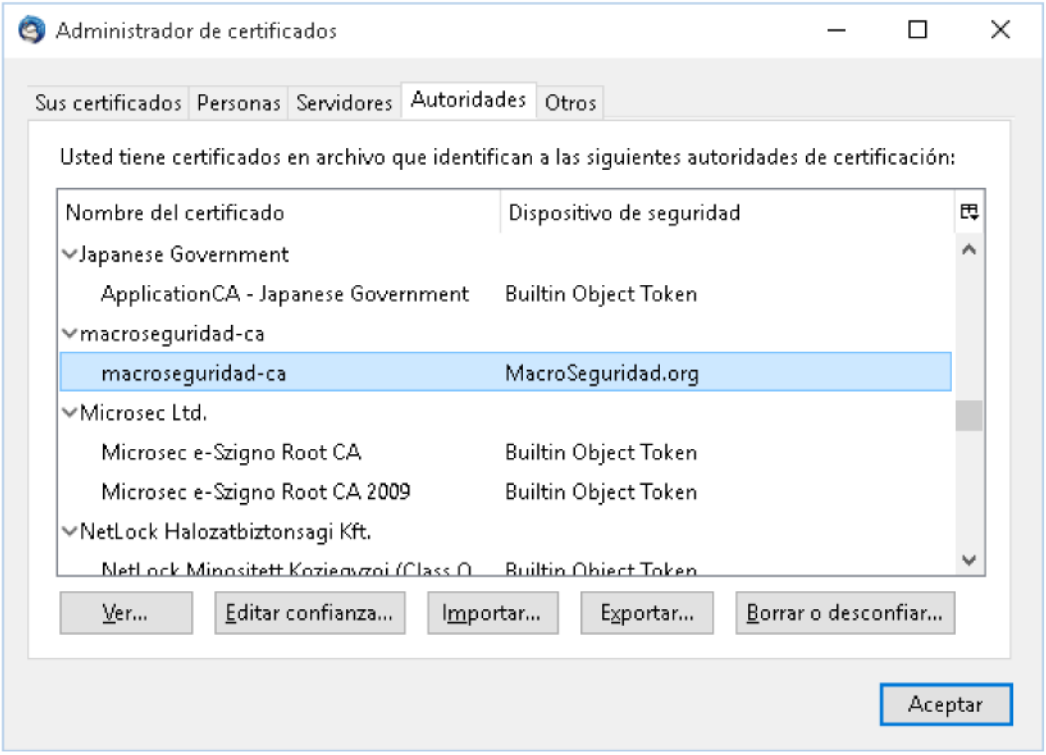
Diríjase al directorio donde este guardado el certificado raíz de la Entidad Certificadora que desea importar, selecciónelo y haga click en "*Abrir*".



A continuación deberá indicar los propósitos para los cuales instalará esta Autoridad de Certificación.

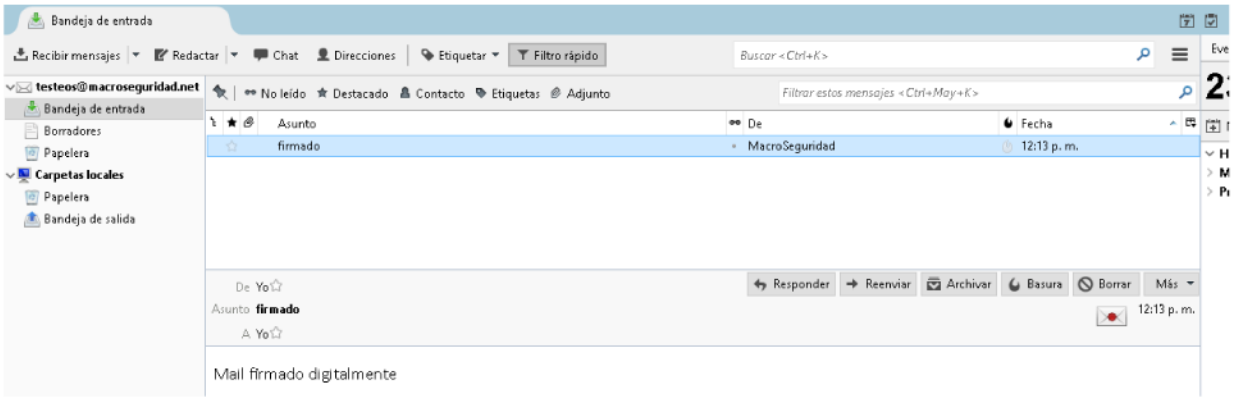


Las opciones mostradas permiten seleccionar en qué instancias usted confía en un certificado emitido por la CA. Una vez importado el certificado se mostrará de la siguiente manera:

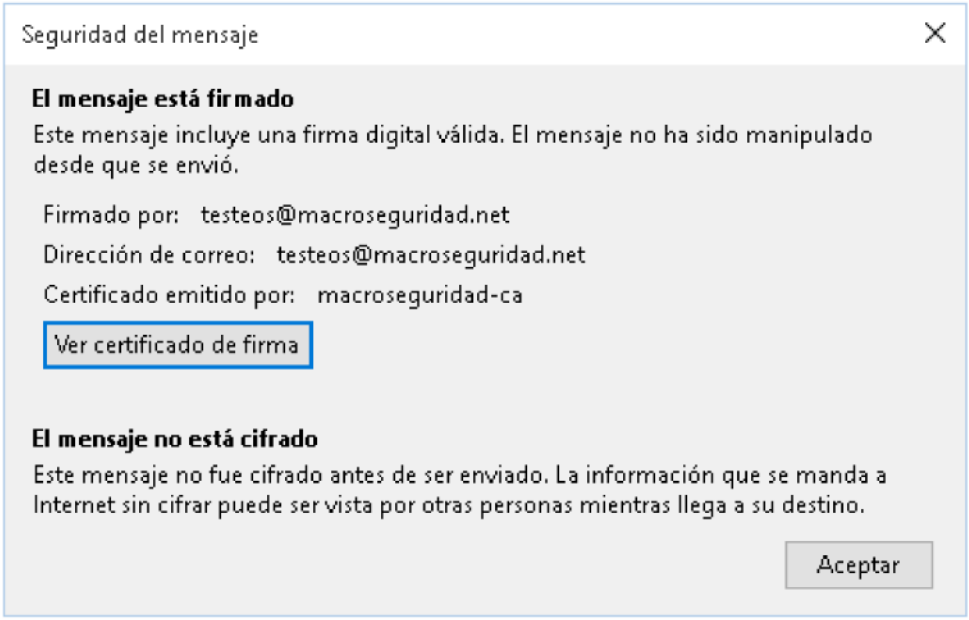


Haga click en "*Aceptar*" para finalizar con el asistente.

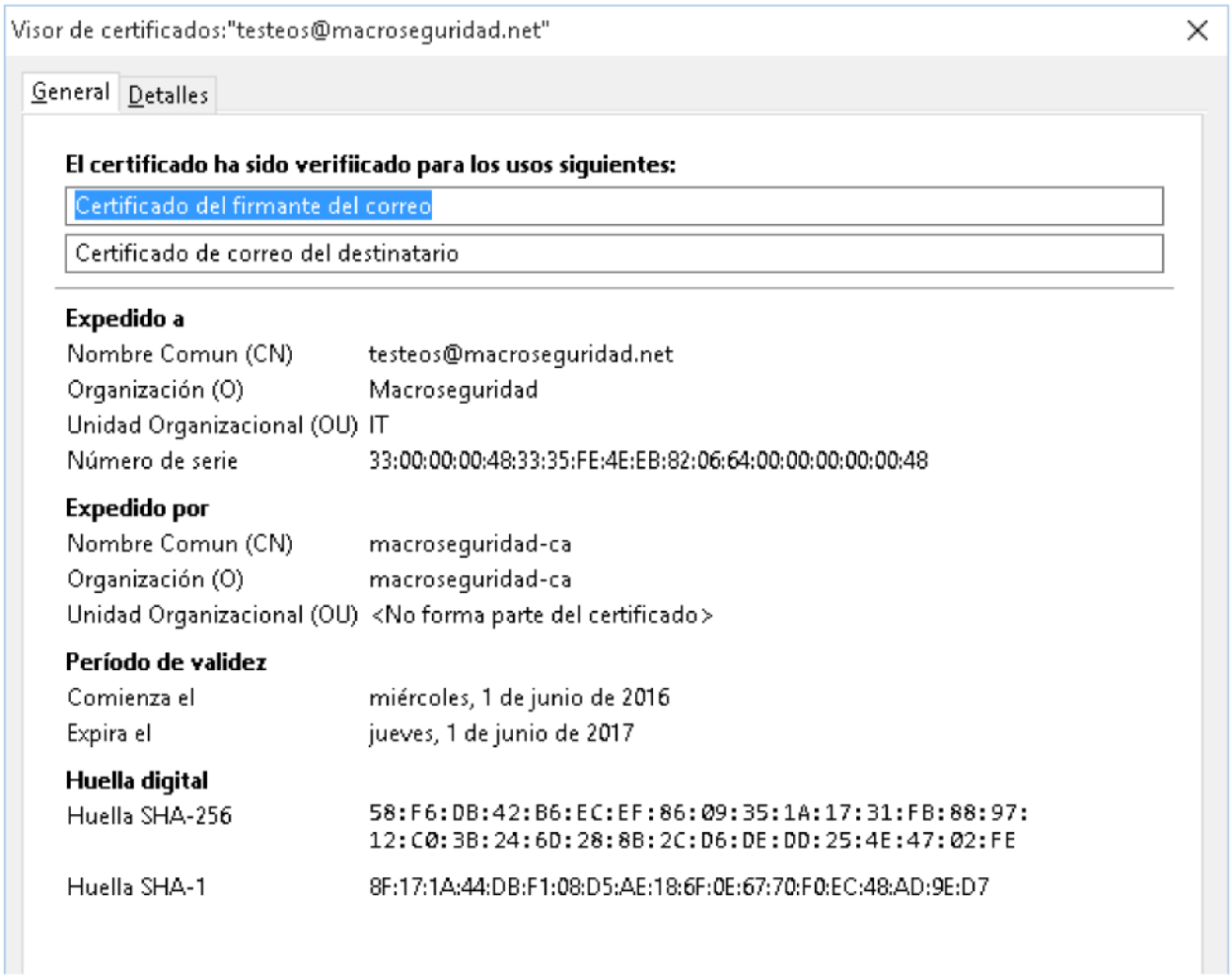
Como podrá observar en la siguiente imagen, el ícono de firma digital que indicaba que la CA no era de confianza ha cambiado e indica que el mail fue firmado por un certificado confiable.



Haga click sobre este y se abrirá una nueva ventana en donde podrá verificar que efectivamente la firma es ahora válida.



Haga click en "*Ver certificado de firma*" y se mostrará una nueva ventana con información detallada del certificado utilizado para la firma digital.



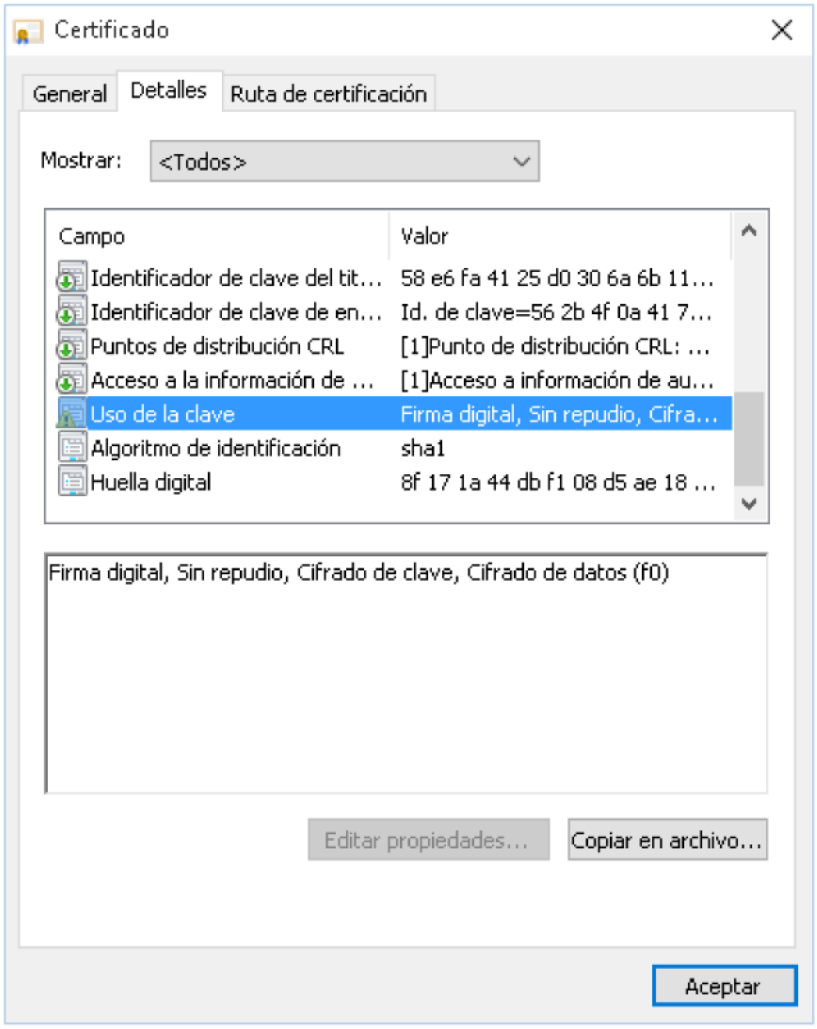
8 Utilizar un MS-IDProtect para Encriptar mails

En la sección anterior se expuso el uso de certificados digitales almacenados dentro del MS-IDProtect para firmar correo. En esta sección se explicará una funcionalidad complementaria a la anterior: la Encripción y Firma de Mails.

La encripción se utiliza desde hace muchos años, con el fin de preservar la confidencialidad de los mensajes (es decir, que sólo sea leído por aquella persona que debe hacerlo). Junto con el uso de la tecnología de firma digital podemos lograr, además de la autenticación, la integridad y el no repudio de los mensajes, la confidencialidad de la información transmitida a través de este medio.

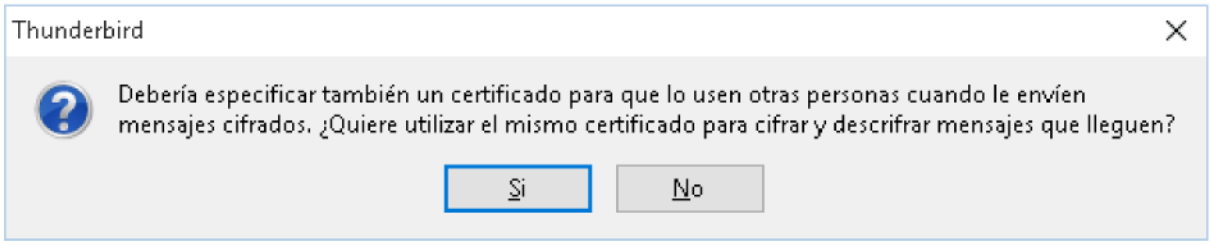
Usted deberá asegurarse que su certificado tenga la funcionalidad de Encripción de Mails.

Para ello tiene que verificar que en "*Uso de la clave*" esté listado la funcionalidad "*Cifrado de clave*" en los detalles del certificado.

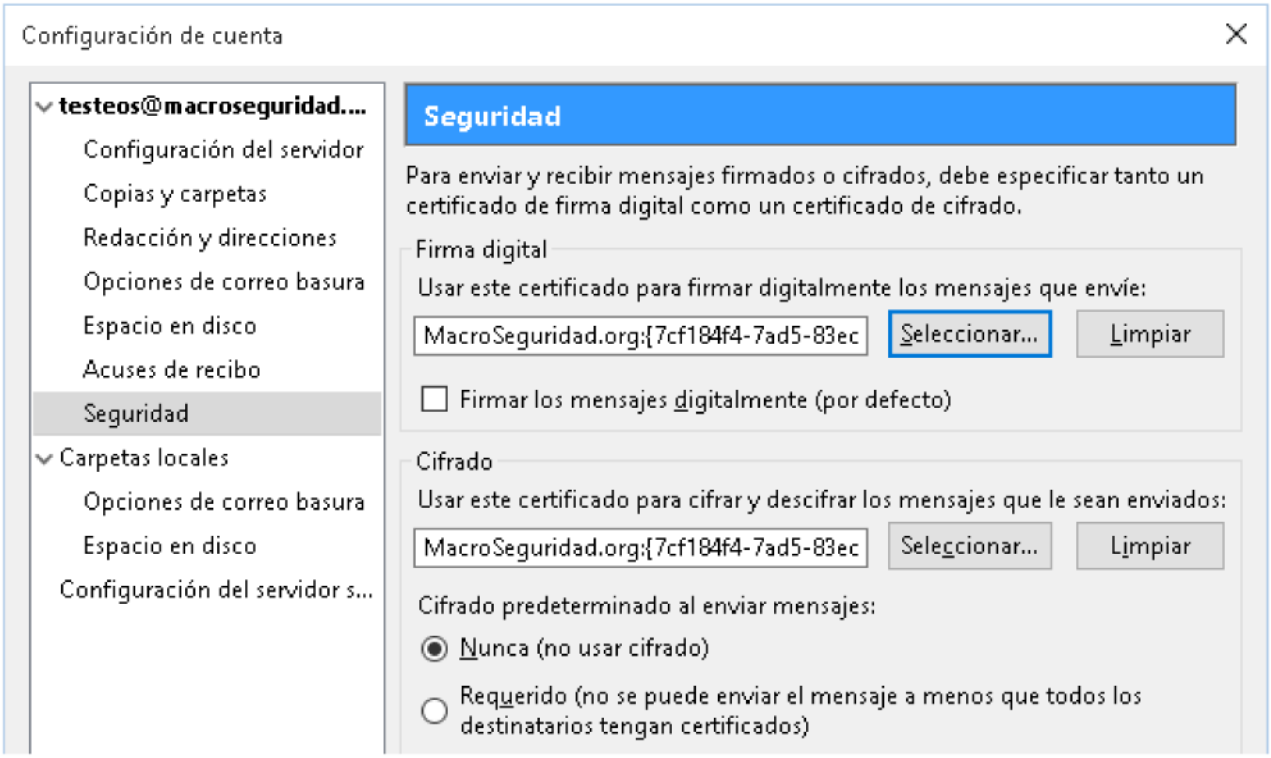


8.1 Configurar un Certificado almacenado dentro de un MS-IDProtect para desencriptar un Mail

En principio, los pasos son los mismos que en la sección 6.2. Deberá asegurarse de haber contestado "*Si*" cuando Thunderbird le pregunte si desea utilizar el mismo certificado para encriptar:



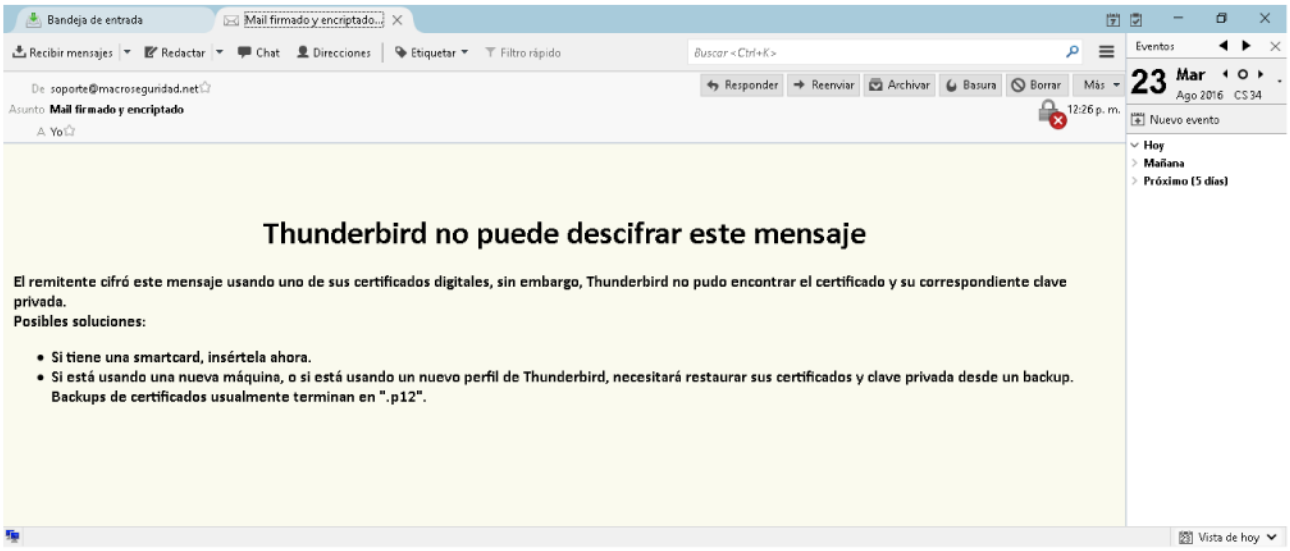
La configuración que se encuentra a continuación bastará para firmar, encriptar y desencriptar los mails que le lleguen cifrados, utilizando el MS-IDProtect y el certificado contenido dentro del mismo.



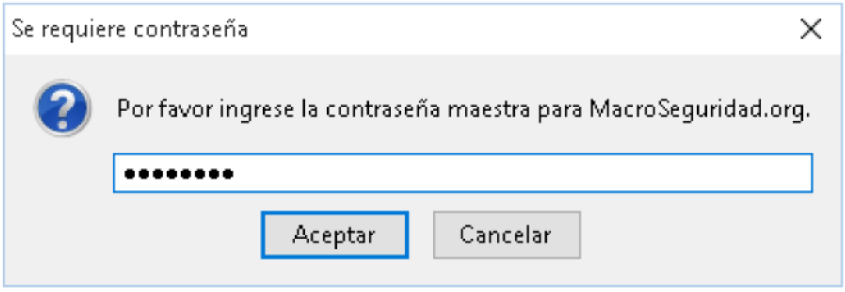
8.2 Desencriptar mails con un MS-IDProtect de Macroseguridad.org

Ud. deberá distribuir la clave pública de su certificado para que sus contactos puedan encriptar los mensajes que le envían. Para hacerlo puede exportar el certificado de su Token/SmartCard y hacer llegar el archivo exportado a sus contactos. La mejor opción es enviarle un mail firmado digitalmente a todos los contactos que Ud. desee.

En la siguiente pantalla, se muestra un mail al momento que el usuario está intentando abrir un mensaje que ha llegado cifrado y el Token USB/SmartCard MS-IDProtect con el certificado correspondiente para desencriptar no está presente:

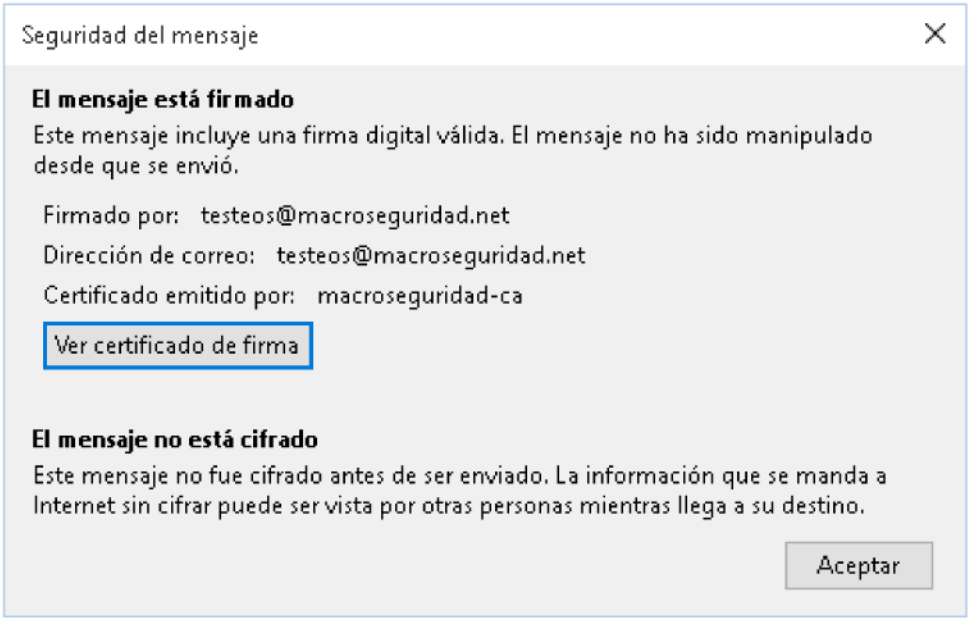


Al conectar el Token USB / SmartCard, le solicitará automáticamente el PIN de Usuario para acceder al mismo:



Una vez ingresado el PIN, el mail será desencriptado utilizando el certificado digital almacenado en el MS-IDProtect, y el contenido del mismo podrá ser leído:

Puede observar que en el mismo mail se muestra el ícono de "*firmado*" y se ha agregado un nuevo icono, el candado de "*cifrado*". Haciendo click en cualquiera de estos íconos, se abrirá la siguiente ventana, mostrando la información correspondiente a la persona que firmó y envió el mail.

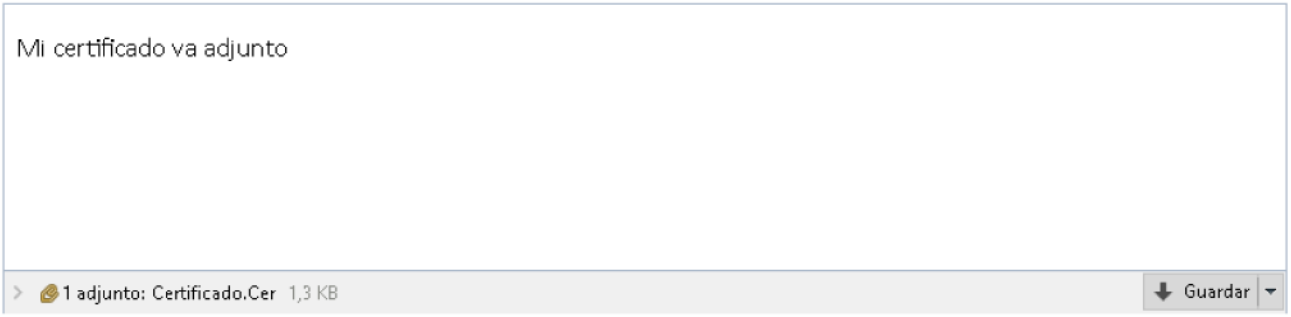


8.3 Obtener el Certificado Digital de Otra Persona

Si desea enviar un mensaje a otra persona, y que este mensaje no sea leído por otros, deberá encriptarlo. Como fue explicado en pasos anteriores, necesitará el certificado digital (clave pública) de la otra persona a la que quiere enviarle el mail protegido.

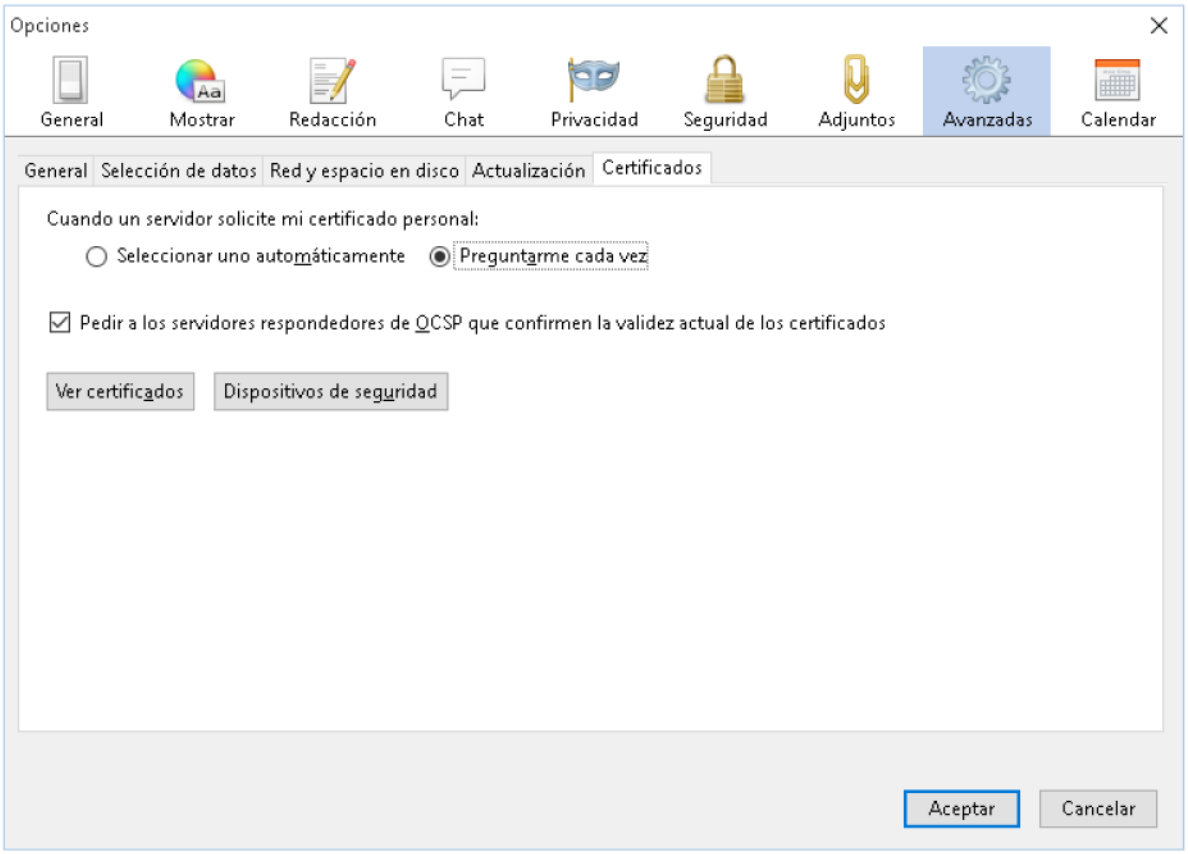
La forma más fácil es a través de un mail firmado del contacto. Para poder vincular este certificado con la persona que mandó el mail, guarde el contacto desde el mail firmado. Para hacer esto, haga click en el botón derecho sobre el remitente y en el menú que se despliega seleccione la opción “Agregar a la libreta de direcciones”

Otra forma, por ejemplo, es enviar el certificado .CER adjunto como se muestra en el siguiente mensaje. El mismo contiene un certificado digital adjunto que corresponde al remitente.

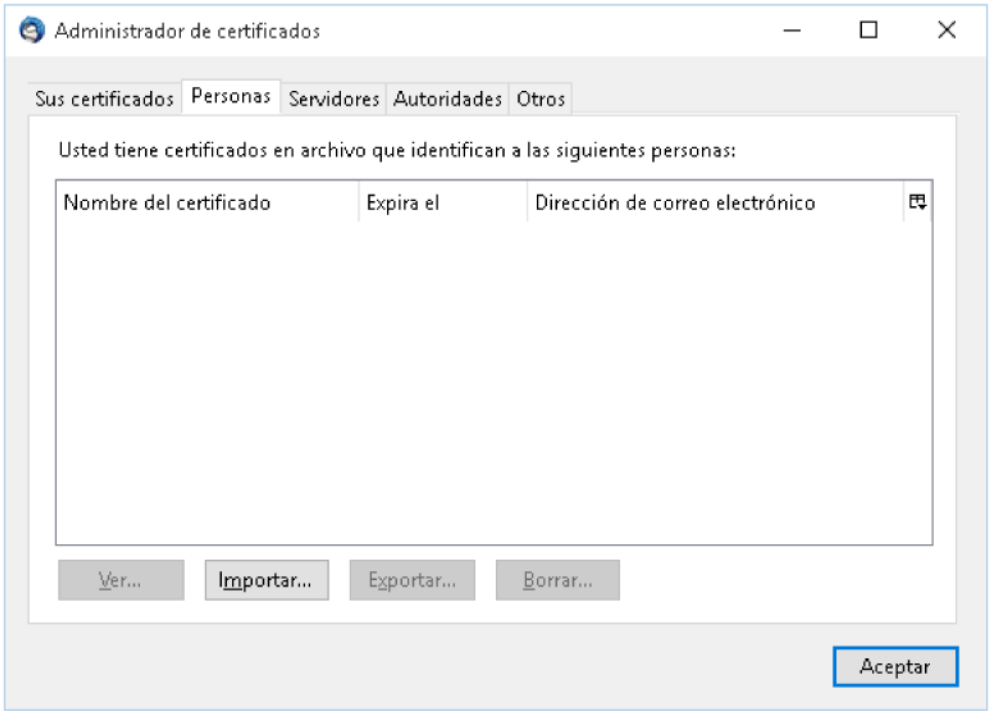


Para importar el certificado a Mozilla Thunderbird primero guarde el certificado en alguna ubicación que recuerde en su PC.

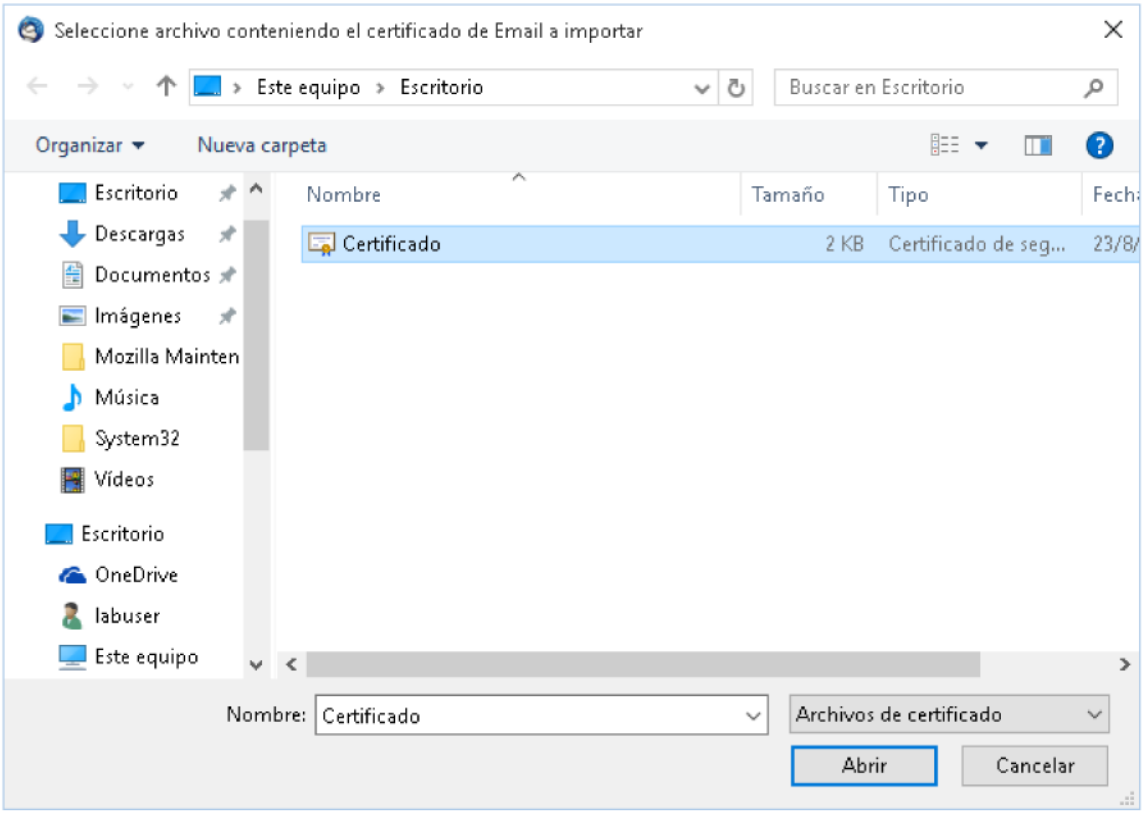
Luego, abra nuevamente la sección de “*Seguridad*”, en el menú “*Avanzadas*” y haga click en “*Ver Certificados*”.



Seleccione la solapa "*Personas*" y haga click en "*Importar*"



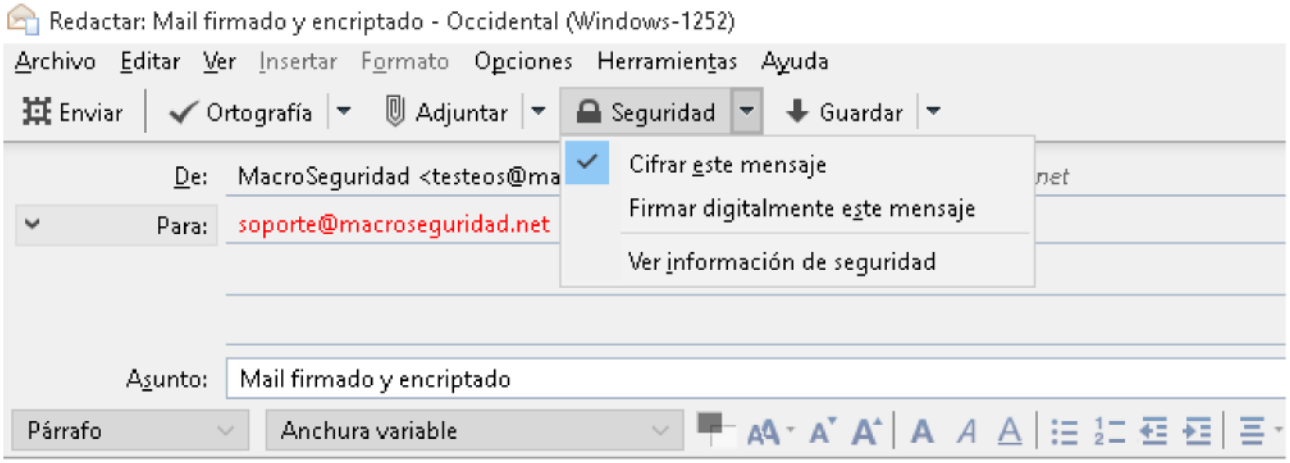
Luego, seleccione el certificado que acaba de guardar y haga click en "*Abrir*".



De esta forma, ya tiene el certificado asociado a la cuenta del remitente (en este caso soporte@macroseguridad.net) por lo que podrá enviarle mensajes encriptados.

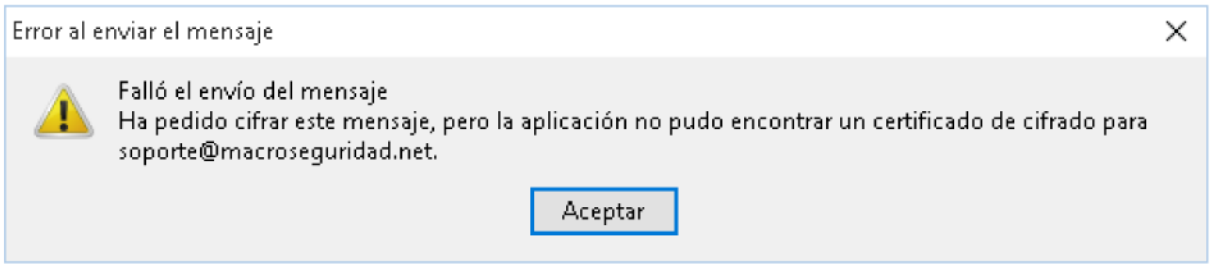
8.4 Enviar un Mail Encriptado

Una vez que tiene el certificado digital asociado a una determinada dirección de correo (como se vio en la sección anterior), Ud. puede encriptar los mensajes que envía a dicha dirección. Complete los campos necesarios y seleccione "Cifrar este mensaje" en la barra de menú de seguridad, como se muestra a continuación.



Luego escriba el contenido del mensaje y haga click en "*Enviar*". El mensaje será encriptado y enviado.

Si no realizó los pasos previos (almacenamiento del certificado del destinatario o agregó el contacto desde el mail firmado), se le mostrará un mensaje como el siguiente, indicando que no tiene la clave para encriptar el mensaje para esa persona.



Para que alguien pueda mandarle mails encriptados a usted, esa persona deberá tener su certificado digital.

Esto se logra simplemente mandando a esa persona un mail firmado digitalmente por usted o con el certificado como archivo adjunto, de esa forma podrá obtener a través de ese mail su certificado.

9 Apéndice 1: Autoridad Certificante (CA)

9.1 Concepto de CA

La **Autoridad Certificante o Certificadora**, por sí misma o mediante la intervención de una Autoridad de Registro, puede verificar la identidad del solicitante de un certificado antes de la emisión del mismo o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Los certificados digitales son la contraparte del documento de identidad de una persona, los mismos incorporan ciertos datos de su titular y su clave pública y están firmados electrónicamente por la **Autoridad Certificante** utilizando su clave privada, la cual está siempre en resguardo bajo estrictas normativas de seguridad.

La **Autoridad Certificante** es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública.

La confianza de los usuarios depositada en la **CA** es importante para el funcionamiento del servicio y justifica la filosofía de su empleo, pero no existe un procedimiento normalizado para demostrar que una CA merece dicha confianza.

Un **certificado revocado** es un certificado que no es válido aunque se emplee dentro de su período de vigencia.

9.2 Contenido del certificado digital

Los componentes más importantes a título informativo de un certificado digital son:

- Clave pública
- Clave privada
- Información del Propietario que vincula el par de claves con la identidad de la persona (estos datos pueden variar según el uso del certificado, y pueden ser nombre y apellido, DNI, mail, pasaporte, etc.)
- Información del emisor del Certificado (nombre de la entidad certificante, clave pública de la misma)
- Información del certificado (período de validez, usos del certificado, etc.)

9.3 Confianza en una CA

Agregar una CA a la lista de confianza es necesario para que nuestra PC acepte operaciones relacionadas a la firma y encripción de emails, y en las que se involucren certificados firmados por esa CA. En el caso de los mails firmados no se hace tan evidente la necesidad de agregar una CA a la lista de confianza, ya que de una u otra forma el mail se puede leer y ver quien lo firmó. En cambio, para utilizar la gran cantidad de características y funcionalidades del Token USB, como por ejemplo Smartcard Logon, comunicarse a través de una VPN (Cisco, Checkpoint, Fortinet; Watchguard, Sonicwall, Microsoft, OpenVPN, etc.), encriptado de datos, es absolutamente necesario tener a la CA incorporada entre las CAs de confianza del sistema.

Básicamente se puede ver como un recordatorio, ya que le decimos a la máquina que recuerde que los certificados de esta CA son confiables. Nos evita el problema de cada vez que llega un certificado, tener que abrirlo para ver qué CA lo firmó y analizar si confiamos en esa CA. Por lo tanto resulta más práctico, rápido y necesario en ciertas ocasiones.

10 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 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