



Firmado y cifrado de mensajes de correo electrónico

Autor: Pedro R. Benito da Rocha <pedro@ubu.es>

Última modificación: 01/07/2022

Requisitos previos.....	2
Cliente Outlook.....	3
Windows.....	3
Lectura de un mensaje firmado.....	3
Envío de un mensaje firmado.....	5
Lectura de un mensaje encriptado.....	5
Envío de un mensaje encriptado.....	6
macOS.....	7
Lectura de un mensaje firmado.....	7
Lectura de un mensaje encriptado.....	7
Envío de un mensaje firmado.....	7
Envío de un mensaje encriptado.....	8
Cliente Mozilla Thunderbird.....	9
Pasos previos.....	9
Configurar certificados raíz.....	9
Configuración del certificado de usuario.....	9
Lectura de mensajes firmados.....	11
Envío de mensajes firmados.....	11
Lectura de mensajes encriptados.....	11
Envío de mensajes encriptados.....	12
Outlook en la web (OWA).....	13
Navegador Edge (solo Windows).....	13
Lectura de mensajes firmados.....	13
Envío de mensajes firmados.....	14
Lectura de mensaje cifrados.....	15
Envío de mensajes cifrados.....	15



Requisitos previos

Para poder enviar un mensaje firmado es necesario:

- Certificado digital asociado a la cuenta de correo. Las pruebas se han hecho con un certificado digital de la FNMT para empleado público. Se puede usar el configurador de la FNMT para instalar los certificados, o se pueden desde cargar desde la página web de la FNMT¹.
- Cliente con capacidad de firmado de correos electrónicos mediante S/MIME usando certificados digitales.

Para poder enviar un mensaje encriptado es necesario:

- Certificado digital asociado a la cuenta de correo. Las pruebas se han hecho con un certificado digital de la FNMT para empleado público.
- Cliente con capacidad de encriptado de correos electrónicos mediante S/MIME usando certificados digitales.
- Certificado del destinatario. Para ello se debe haber intercambiado el certificado (parte pública), por ejemplo enviando un mensaje firmado.

Para poder leer un mensaje firmado:

- Cliente con capacidad de leer mensajes firmados con S/MIME.
- Certificado raíz de la entidad certificadora configurado para su uso en correo electrónico.

Para poder leer un mensaje encriptado:

- Cliente con capacidad de leer mensajes encriptados con S/MIME.
- Certificado raíz de la entidad certificadora configurado para su uso en correo electrónico.
- Certificado (parte pública) del remitente.

¹ <https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt>

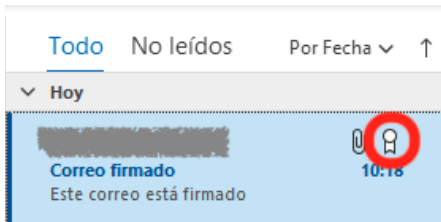


Ciente Outlook

Windows

Lectura de un mensaje firmado

Los correos firmados se distinguen por una insignia que indica esta circunstancia.



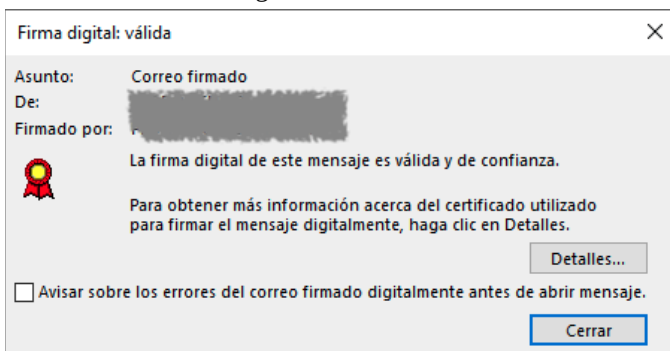
Al abrir el mensaje aparece la insignia a color en la parte superior derecha.

Correo firmado



Este correo está firmado digitalmente.

Haciendo clic en la insignia se muestra la información relativa a la validez de la firma del mensaje.



Para que una firma válida sea reconocida tan solo es necesario que el certificado raíz del remitente esté instalado en el almacén de certificados del sistema. El certificado raíz debe tener activada la función "Correo seguro". Muchas de las firmas digitales ya están reconocidas por el sistema, pero en algunos casos es necesario indicar al sistema que debe usar para correo seguro los certificados que tiene instalados.

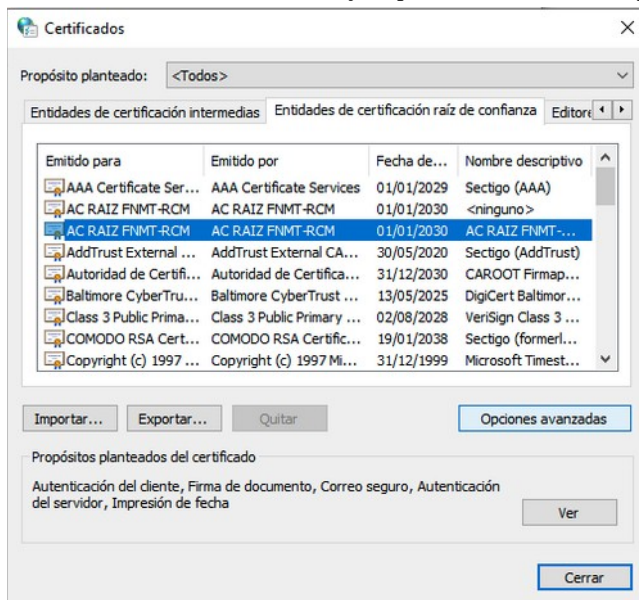
Los certificados personales que ofrece la FNMT a los ciudadanos y los certificados de empleado público necesitan la configuración que vamos a describir a continuación.

Para utilizar los certificados de la FNMT se puede usar el configurador que se descarga desde <https://www.sede.fnmt.gob.es/descargas/descarga-software/instalacion-software-generacion-de-claves>. Este programa hay que ejecutarlo con permisos de administrador.

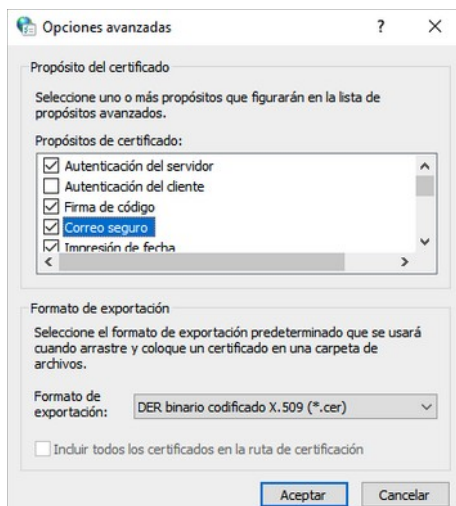


El configurador instalará los certificados, tras lo cual debemos activar su uso para el correo seguro como se ha descrito anteriormente.

Desde Opciones de Internet > Contenido > Certificados se seleccionará la pestaña en la que se encuentre el certificado raíz, se seleccionará y se pulsará en el botón “Opciones avanzadas”.



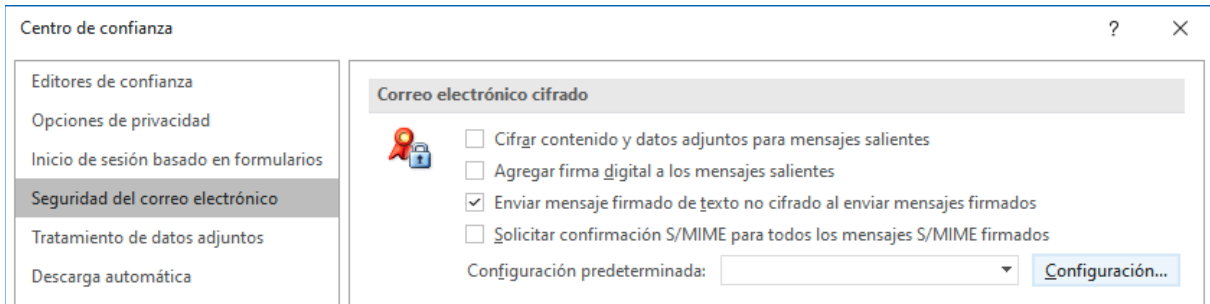
Aparecerá un cuadro de diálogo en el que hay que marcar la opción “Correo seguro”, y luego aceptar los cambios.



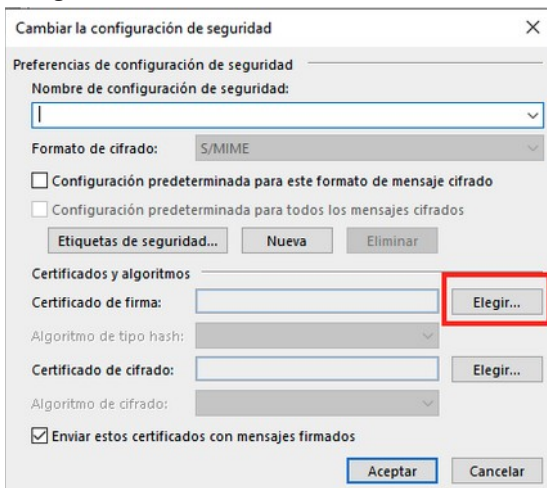


Envío de un mensaje firmado

Antes de poder enviar correos firmados y/o encriptados se debe configurar el certificado digital a utilizar. Para ello hay que ir a Archivo > Opciones > Centro de confianza > Configuración del Centro de confianza > Seguridad del correo electrónico.

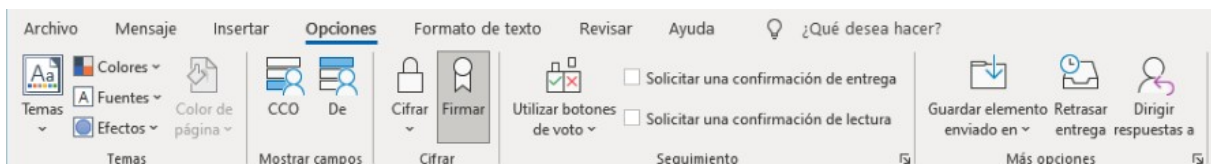


Hay que elegir la configuración predeterminada con el botón “Configuración”, donde podemos elegir el certificado digital a usar, en el caso de tener varios. Para seleccionar los certificados se debe pulsar el botón “Elegir”.



Aquí podemos elegir “Agregar firma digital a los mensajes salientes” si queremos que se firmen todos los mensajes salientes. Si queremos firmar de forma manual cada uno de los mensajes que enviamos, no hay que marcar esta casilla.

La firma manual de los mensajes se realiza desde Nuevo correo electrónico > Opciones > Firmar.



Ahora al enviar el mensaje éste estará firmado.

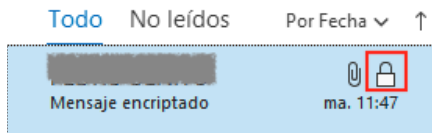
Lectura de un mensaje encriptado

Es necesario haber intercambiado previamente un mensaje firmado por nosotros para que el remitente pueda cifrarlo. Si hemos recibido un mensaje firmado por la persona que nos envía el correo encriptado, y a su vez hemos enviado un correo firmado por nosotros, ambos podremos intercambiar correos encriptados.



Nota: El correo encriptado solamente se puede leer desde el cliente de correo en el que previamente hemos guardado la clave pública de la otra persona.

Los mensajes encriptados aparecen marcados con un candado en la lista de mensajes.

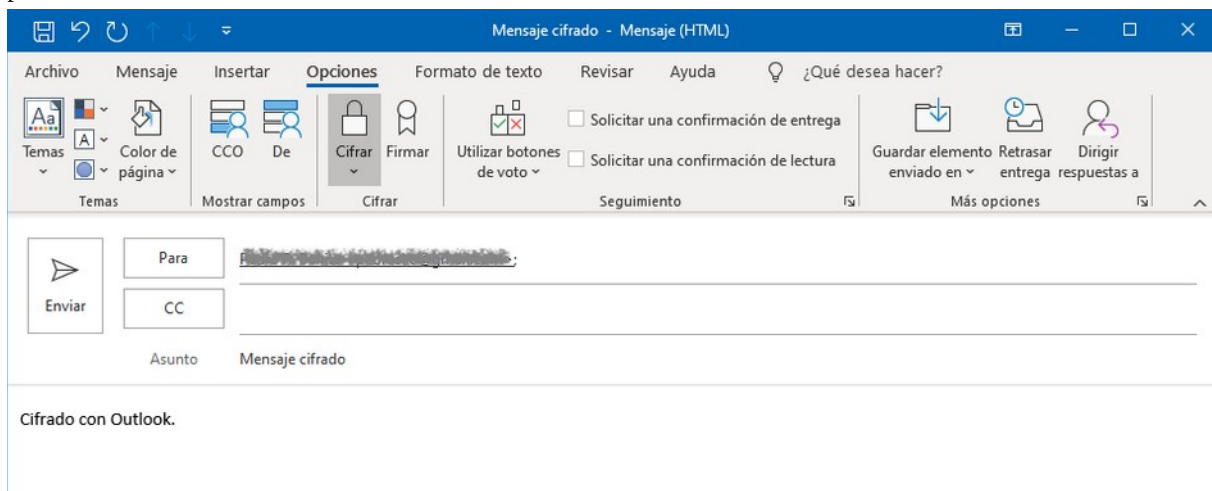


Esto indica que el emisor ha enviado el mensaje encriptado y solamente lo podemos desencriptar nosotros. Los mensajes encriptados aparecen en el panel de lectura con un candado.

Envío de un mensaje encriptado

Para enviar un mensaje encriptado es necesario haber recibido previamente un mensaje firmado de la persona a la que se va a enviar el mensaje encriptado.

Desde la cinta seleccionamos Opciones > Cifrar. El mensaje se enviará encriptado y solamente el destinatario podrá acceder a su contenido.

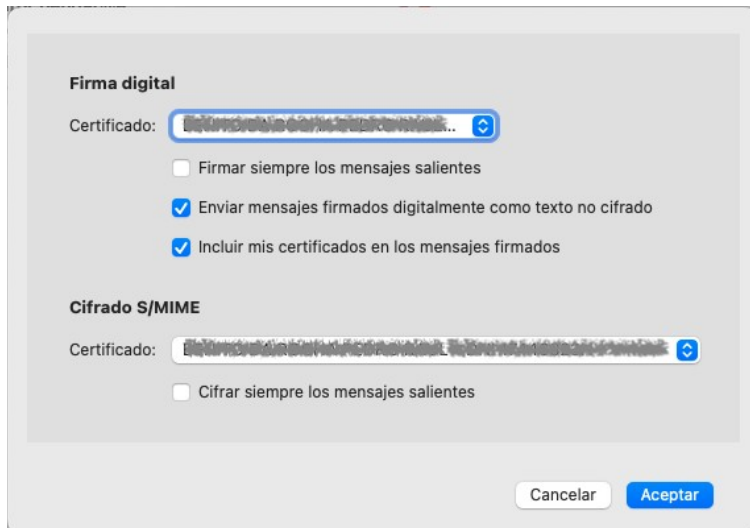




macOS

El cliente Microsoft Outlook de macOS está disponible a través de la suscripción A3 de Office 365.

Para poder utilizar las capacidades de firmado y encriptado primero hay que tener instalado el certificado digital en el ordenador. Una vez instalado se ha de ir a Preferencias > Cuentas, elegir la cuenta (si hubiera varias) y seleccionar el botón “Seguridad” del panel de la derecha, abriéndose un cuadro de diálogo en que se ha de elegir el certificado para la firma y para el encriptado de correo:



En este mismo cuadro de diálogo se puede elegir firmar y/o cifrar todos los mensajes salientes.

Lectura de un mensaje firmado

Tan solo es necesario que el certificado raíz del remitente esté instalado en el llavero del sistema.

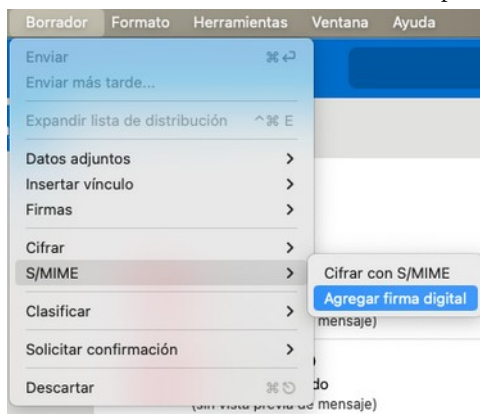
Lectura de un mensaje encriptado

Es necesario haber intercambiado previamente un mensaje firmado por nosotros para que el remitente pueda cifrarlo. No es necesaria ninguna acción especial por parte nuestra.

Envío de un mensaje firmado

Para enviar un mensaje firmado se ha de disponer de un certificado como se ha indicado previamente.

Se utiliza el botón “Nuevo mensaje” como si fuéramos a redactar un correo normal y corriente. Si no se ha seleccionado “Cifrar siempre los mensajes salientes” en el cuadro de diálogo de la configuración de los certificados será necesario, desde la composición del mensaje, ir al menú Borrador > S/MIME:





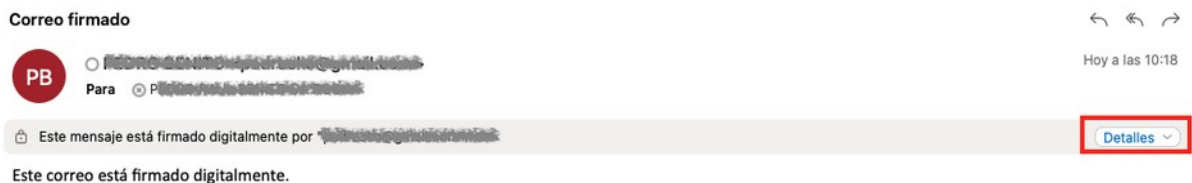
Desde la opción “Agregar firma digital” se indica que se desea firmar el mensaje.

Esta operación hay que realizarla ANTES de escribir los destinatarios del mensaje, o no aparecerá en el menú.

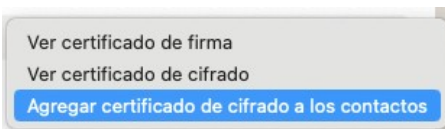
Una vez redactado el mensaje y añadidos los destinatarios es posible que se nos solicite varias veces las credenciales de inicio de sesión para acceder al llavero. Esto es necesario ya que macOS protege el llavero donde se almacenan los certificados para evitar accesos no autorizados a las claves.

Envío de un mensaje encriptado

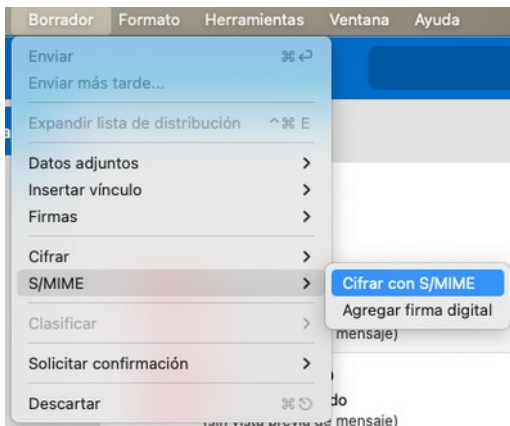
Para enviar un mensaje encriptado primero hay que disponer del certificado (parte pública) del destinatario. Este certificado se obtiene de un mensaje firmado que nos haya enviado previamente.



Desde el mensaje firmado, se selecciona Detalles > Agregar certificado de encriptado a los contactos. Ahora ya se puede enviar correo encriptado con éste usuario.



Si ya tenemos añadido el certificado, utilizamos el botón “Nuevo mensaje” como si fuéramos a redactar un correo normal y corriente. Si no se ha seleccionado “Cifrar siempre los mensajes salientes” en el cuadro de diálogo de la configuración de los certificados será necesario, desde la composición del mensaje, ir al menú Borrador > S/MIME y seleccionar “Cifrar con S/MIME”:



El mensaje se enviará encriptado y solamente podrá abrirlo el destinatario.



Cliente Mozilla Thunderbird

Pasos previos

Configurar certificados raíz

Mozilla Thunderbird soporte S/MIME, tanto para enviar correo como para recibir.

Como paso previo, para que se pueda reconocer la firma de los mensajes es necesario que el certificado raíz del emisor esté instalado y además su uso para correo electrónico esté activado. Desde las preferencias de Thunderbird accedemos a “Privacidad y Seguridad” > Seguridad > Certificados, y elegimos el botón “Administrar certificados”.

Certificados

Cuando un servidor solicite mi certificado personal:

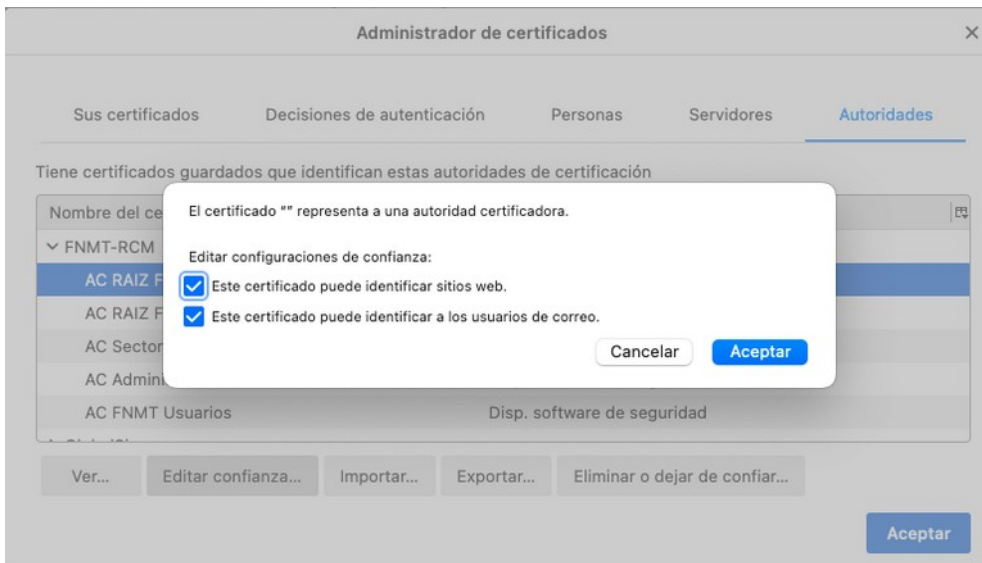
Seleccionar uno automáticamente Preguntarme cada vez

Preguntar a los servidores respondedores de OCSP para confirmar la validez actual de los certificados

Administrar certificados...

Dispositivos de seguridad...

Buscamos el certificado raíz en “Autoridades” y pulsamos el botón “Editar confianza”:



Por último, seleccionamos “Este certificado puede identificar a los usuarios de correo.” y Pulsamos “Aceptar”. Ahora Thunderbird ya puede utilizar correctamente el certificado.

Configuración del certificado de usuario

Thunderbird utiliza su propio almacén de certificados, por lo que instalar un certificado en el sistema operativo (por ejemplo, en Windows, usando las opciones de Internet) no sirve para utilizar correo seguro en Thunderbird.

Desde las preferencias de Thunderbird vamos a “Configuración de la cuenta”. Seleccionaremos la cuenta que deseamos configurar e iremos a la sección “Cifrado extremo a extremo”. En la sección S/MIME debemos importar y seleccionar el certificado de usuario que queremos utilizar.



Para importar el certificado hacemos clic en el botón “Administrar certificados S/MIME”, buscamos el fichero con el certificado y lo importamos.

S/MIME
Certificado personal para la firma digital:

Certificado personal para cifrado:

Configuración predeterminada para el envío de mensajes
Sin cifrado de extremo a extremo los contenidos del mensaje quedan expuestos fácilmente a su proveedor de correo y a la vigilancia masiva.

No activar cifrado por defecto
 Requerir cifrado por defecto

Si necesita cifrado, para enviar un mensaje debe tener la clave pública o certificado de cada destinatario.

Una firma digital permite a los destinatarios verificar que el mensaje fue enviado por usted y que el contenido no ha sido modificado.

Añadir mi firma digital de forma predeterminada

Administrador de certificados

Sus certificados | Decisiones de autenticación | Personas | Servidores | Autoridades

Tiene certificados de estas organizaciones que le identifican

Nombre del certificado	Dispositivo de seguridad	Número de serie	Caduca el
------------------------	--------------------------	-----------------	-----------

A continuación, debemos usar el botón “Seleccionar” para elegir el certificado que deseamos utilizar.

S/MIME
Certificado personal para la firma digital:

Certificado personal para cifrado:

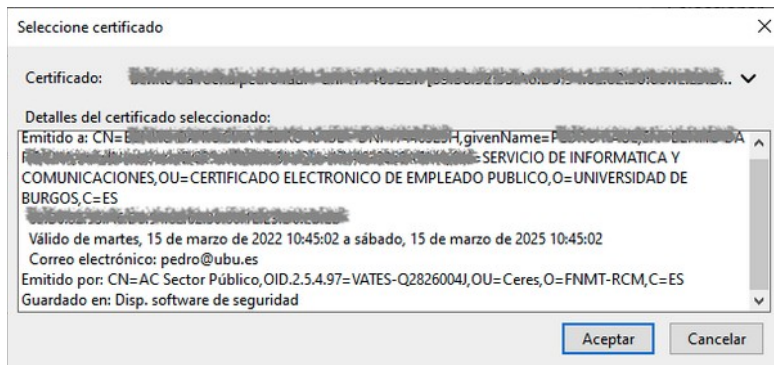
Configuración predeterminada para el envío de mensajes
Sin cifrado de extremo a extremo los contenidos del mensaje quedan expuestos fácilmente a su proveedor de correo y a la vigilancia masiva.

No activar cifrado por defecto
 Requerir cifrado por defecto

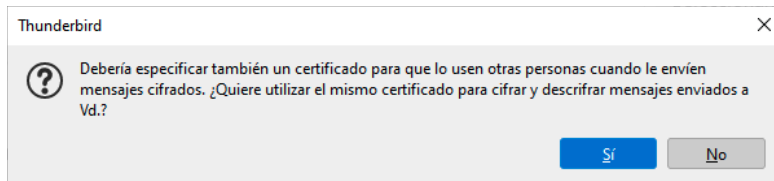
Si necesita cifrado, para enviar un mensaje debe tener la clave pública o certificado de cada destinatario.

Una firma digital permite a los destinatarios verificar que el mensaje fue enviado por usted y que el contenido no ha sido modificado.

Añadir mi firma digital de forma predeterminada



Thunderbird nos sugiere usar el mismo certificado para los mensajes encriptados. Si vamos a usar esta característica contestamos “Sí”.



Lectura de mensajes firmados

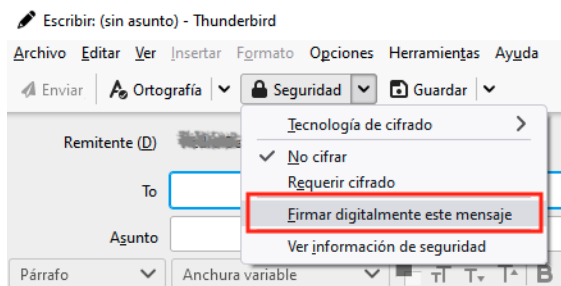
Si se han seguido los pasos previos, Mozilla Thunderbird reconocerá los mensajes firmados, y en el caso de que la firma sea correcta se mostrará un icono en la parte derecha del encabezado indicando esta situación.



Haciendo clic en el icono se puede obtener más información sobre la firma del mensaje.

Envío de mensajes firmados

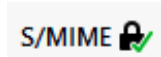
Para enviar un mensaje firmado basta con usar la opción Seguridad > Firmar digitalmente este mensaje al redactar el mensaje.



El mensaje será firmado cuando pulsemos el botón “Enviar”.



Lectura de mensajes encriptados

Los mensajes encriptados que pueden ser leídos correctamente tiene éste icono en la parte derecha del encabezado:



Un correo puede estar cifrado y firmado, con lo que aparecen los dos iconos:



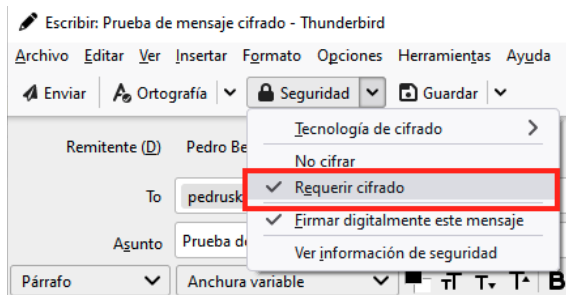
S/MIME  

Para que un mensaje encriptado pueda ser leído es necesario haber intercambiado con el remitente al menos un correo firmado. De esta forma ambos intervinientes tienen la información necesaria para poder cifrar y descifrar el mensaje.

Envío de mensajes encriptados

Como paso previo deberemos haber recibido correctamente un mensaje firmado por el remitente.

Desde la redacción del mensaje seleccionamos la opción Seguridad > Requerir cifrado.



Este mensaje está cifrado con Thunderbird.

Si todo está correcto, se enviará el mensaje cifrado.



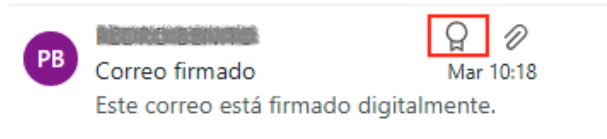
Outlook en la web (OWA)

Navegador Edge (solo Windows)

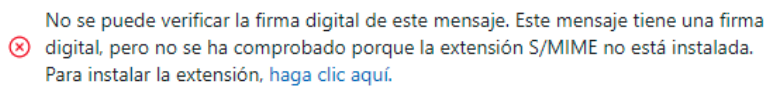
Para poder acceder a la firma y cifrado de mensajes es necesario tener la última versión del navegador Edge.

Lectura de mensajes firmados

Los correos firmados se distinguen por una insignia que indica esta circunstancia.



Por defecto, el navegador no soporta la comprobación de mensajes firmados. Para poder procesar la firma de los mensajes hay que instalar una extensión en el navegador. Esta circunstancia se indica con el siguiente mensaje:



Al hacer clic en el enlace se accede a la página de descarga del complemento de Edge para S/MIME². Las funcionalidades de S/MIME requieren la instalación de una extensión y de un control.



Una vez estemos en la página de descargas se debe pulsar el botón “Obtener”.



Cuando se solicite debemos pulsar el botón “Agregar extensión”.

Una vez instalada la extensión refrescamos la página (pulsando F5 o usando el botón de recargar del navegador).

Al acceder al mensaje aparece un nuevo aviso, indicando que es necesario instalar S/MIME. Esto es normal, ya que Edge usa la extensión del navegador para comunicarse con el control, que es quien procesa la firma del mensaje. Por lo tanto, la extensión por sí sola no es suficiente y debemos instalar también el control a través del enlace que aparece en el aviso:

² S/MIME es un estándar para la firma y cifrado de mensajes de correo electrónico.



⊗ Este mensaje tiene una firma digital, pero no se comprobó porque el control S/MIME no está instalado. Para instalar S/MIME, [haga clic aquí](#).

Al hacer clic se descargará el control para ser instalado.



Seleccionamos “Abrir archivo” desde el botón de descargas y esperamos pacientemente a que se instale. Una vez instalado (no avisa cuando acaba) refrescamos la página y ya podemos comprobar la firma del mensaje.

Los mensajes con firma digital se muestran con un mensaje informativo:

🔔 La firma digital para <[redacted]> en este mensaje es válida y de confianza. Para obtener más información, [haga clic aquí](#).

En el caso de aparecer este otro mensaje:

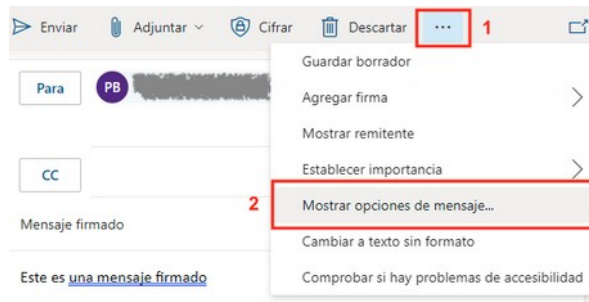
⊗ La firma digital de este mensaje no es válida ni de confianza. Para obtener más información, [haga clic aquí](#).

significará que la firma no puede ser comprobada, y por lo tanto se considera no válida por OWA.

(Nota: Esto no significa necesariamente que la firma no sea válida, puede ser que el certificado para comprobar la firma no se haya subido al tenant de Office 365, lo cual debe hacer un administrador.)

Envío de mensajes firmados

Para enviar un mensaje firmado, redactamos el mensaje como cualquier otro, y al final del proceso debemos acceder al menú de opciones del mensaje (icono con tres puntos) y luego seleccionar “Mostrar opciones del mensaje”:



En el cuadro de diálogo que aparece debemos marcar “Firmar digitalmente este mensaje /S/MIME)” y pulsar en el botón “Aceptar”.

Opciones de mensaje

Confidencialidad
Normal

Solicitar confirmación de lectura

Solicitar una confirmación de entrega

Cifrar este mensaje (S/MIME)

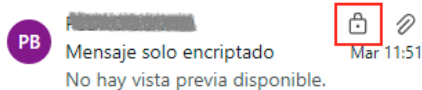
Firmar digitalmente este mensaje (S/MIME)



En la parte derecha de la línea del asunto debe aparecer el icono con la insignia que indica que el mensaje se firmará digitalmente.

Lectura de mensaje cifrados

Los mensajes cifrados se muestran en la lista de mensajes con el icono de un candado para indicar que están cifrados y solamente pueden ser abiertos por el destinatario.



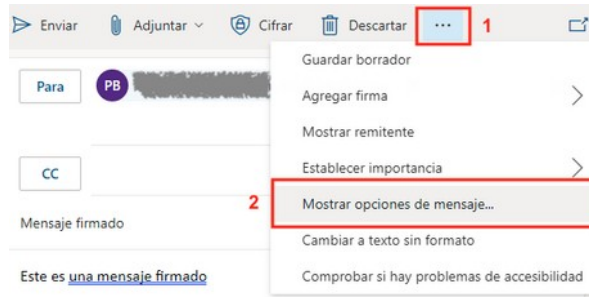
Para poder leer los mensajes cifrados es necesario tener instalado el certificado digital personal correspondiente. Si se tiene el certificado instalado el mensaje se mostrará con un icono adicional de un candado:



Envío de mensajes cifrados

IMPORTANTE: solamente se pueden enviar mensajes cifrados a personas de la propia organización de las que tengamos almacenado su certificado digital (clave pública) en la libreta de direcciones.

Para enviar un mensaje cifrado, redactamos el mensaje como cualquier otro, y al final del proceso debemos acceder al menú de opciones del mensaje (icono con tres puntos) y luego seleccionar “Mostrar opciones del mensaje”:



En el cuadro de diálogo que aparece debemos marcar “Cifrar este mensaje (S/MIME)”.

Opciones de mensaje

Confidencialidad

Normal

Solicitar confirmación de lectura

Solicitar una confirmación de entrega

Cifrar este mensaje (S/MIME)

Firmar digitalmente este mensaje (S/MIME)

Aceptar Cancelar

Opcionalmente también podemos marcar “Firmar digitalmente este mensaje (S/MIME)” para agregar una firma digital al mensaje cifrado.

Una vez elegidas las opciones pulsamos el botón “Aceptar”.

En la parte derecha de la línea del asunto debe aparecer el icono con un candado que indica que el mensaje se cifrará.