Cifrado y firmado de correo electrónico con Mozilla Thunderbird

El presente documento se basa en la versión 24.3 del software Mozilla Thunderbird, siendo esta la versión mínima recomendada para el cifrado/firmado de correo electrónico. Por cuestiones de seguridad, recomendamos que se cuente con la última versión del software en su dispositivo.

También recomendamos proteger su equipo con una contraseña de acceso segura, pues en caso de robo del dispositivo dicho aparato cuenta en su interior con su certificado digital personal, de especial valor.

Instalación del certificado raíz de la FNMT

El primer paso a realizar es la instalación del certificado raíz de la Fábrica Nacional de Moneda y Timbre (en adelante FNMT). Si ya se cuenta con el certificado raíz de la FNMT, no es necesario volverlo a instalar.

En caso de no poseer el certificado raíz de la FNMT, para obtener dicho certificado hay que visitar con el navegador Firefox la página web de la Sede Electrónica de la Universidad de Sevilla, o bien directamente acceder a este enlace directo.,

Si lo desea también lo puede obtener directamente desde el sitio web de la FNMT Descargue los siguientes certificados raíces en su disco duro.

Descarga certificado FNMT Clase 2 CA

Descarga AC Raíz FNMT-RCM

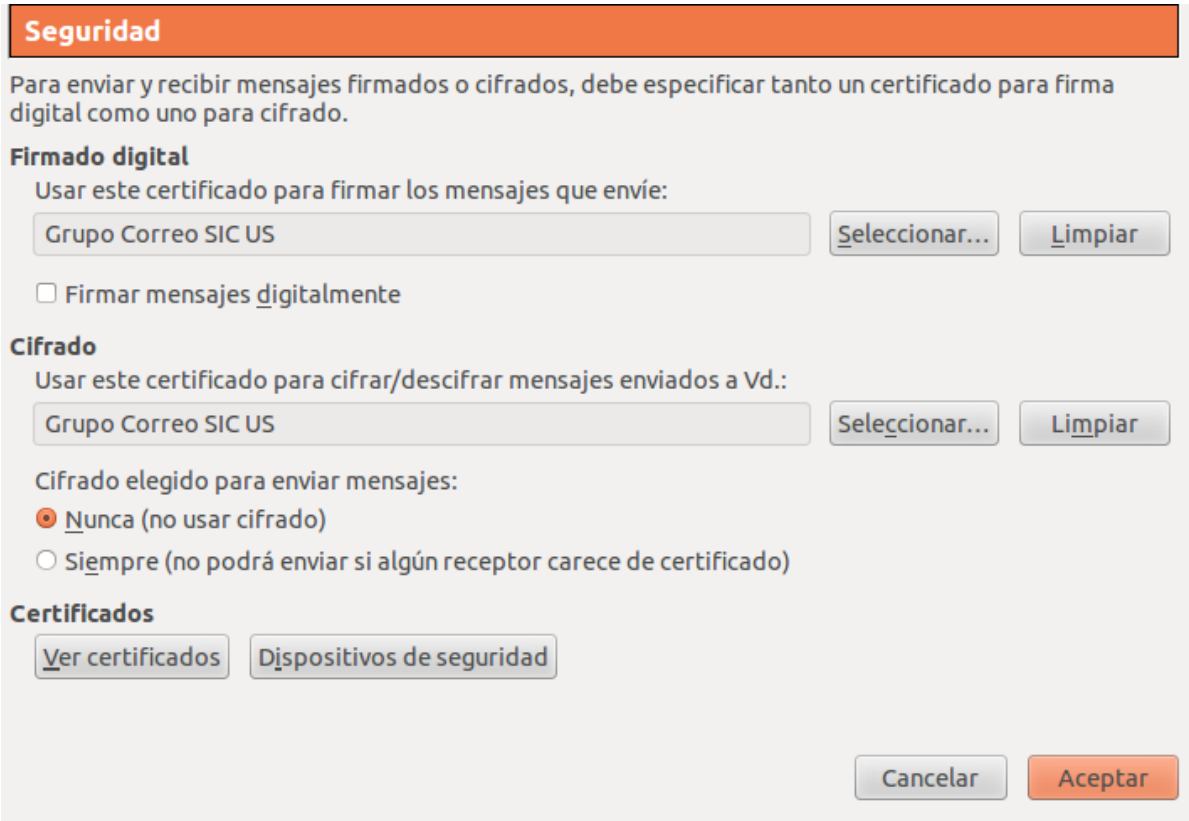
Si va a hacer uso del certificado del DNI electrónico Descarga Certificado AC raíz DNIe .Este certificado va comprimido, deberá descomprimirlo para poder instalarlo.

Una vez descargados los tres certificados:

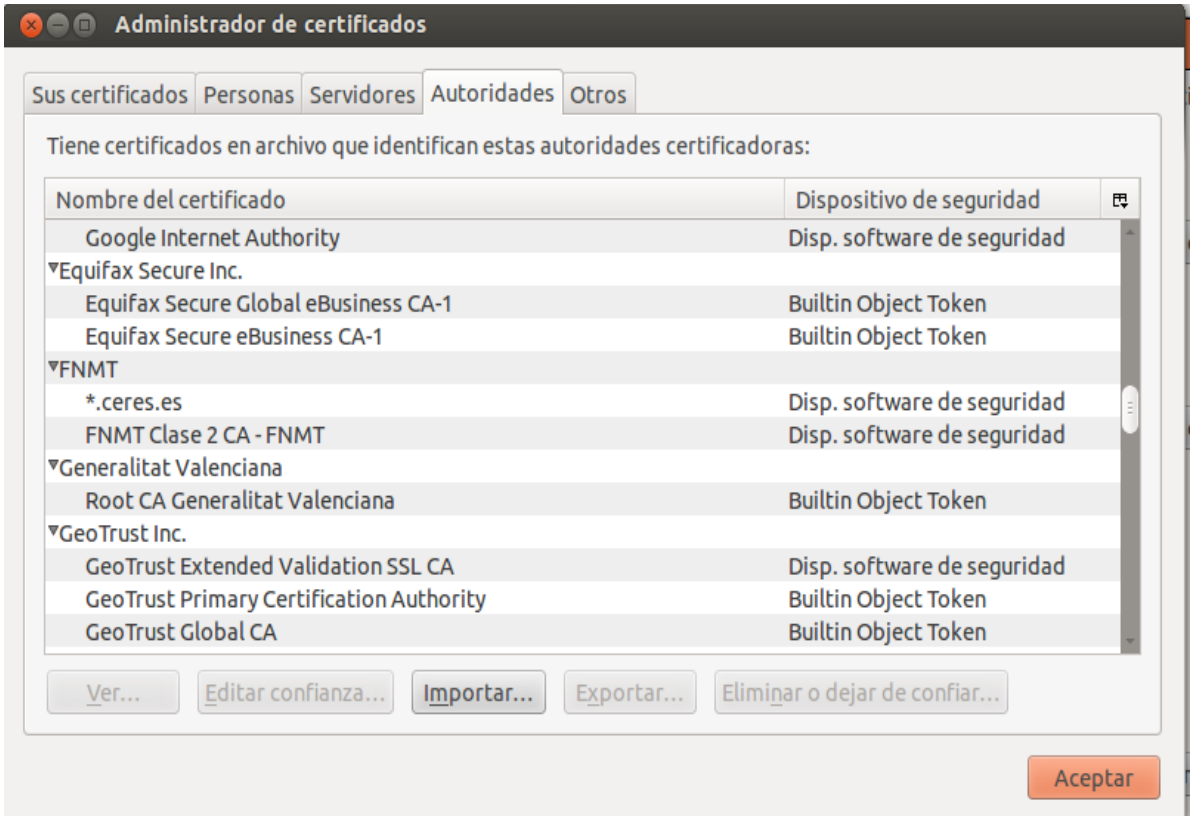
Abra el menú **editar** y en él escoja la opción **configuración de cuentas ...** si su sistema operativo es Linux, o bien, abra el menú **Herramientas** y en él escoja la opción **configuración de las cuentas ...** si su sistema operativo es Windows o MAC. le aparece una ventana de dialogo donde aparece su cuenta y la opción **seguridad** que deberá escoger para pasar a la pantalla donde podrá introducir los

ajustes de seguridad incluyendo lo relativo a certificados para firmado y/o cifrado.

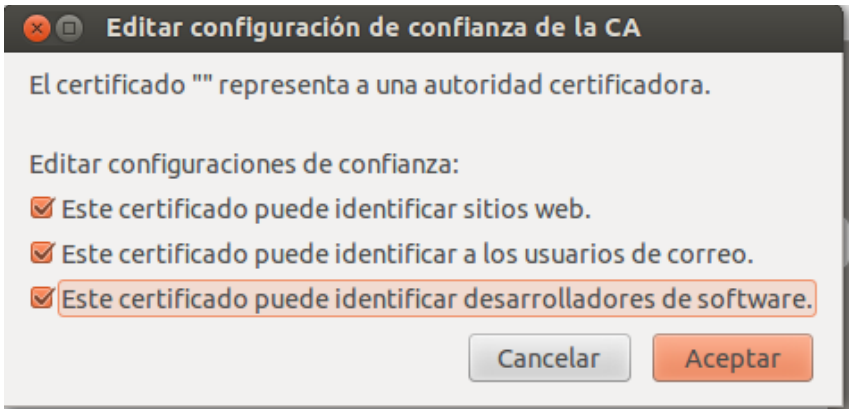
Haga clik el botón **ver certificados**



Seleccione la pestaña **autoridades** y en ella compruebe que aparece el **certificado de autoridad de la FNMT** como se muestra en la imagen, y si no es así, haga click en el botón importar y seleccione el certificado que obtuvo en los pasos anteriores (probablemente un fichero con extensión .CRT) , acepte y se instalará.



Con el **botón editar confianza** podrá indicar los usos que hará del certificado, en el caso que nos ocupa como mínimo deberá marcar **Confiar en esta CA para identificar usuarios de correo** .



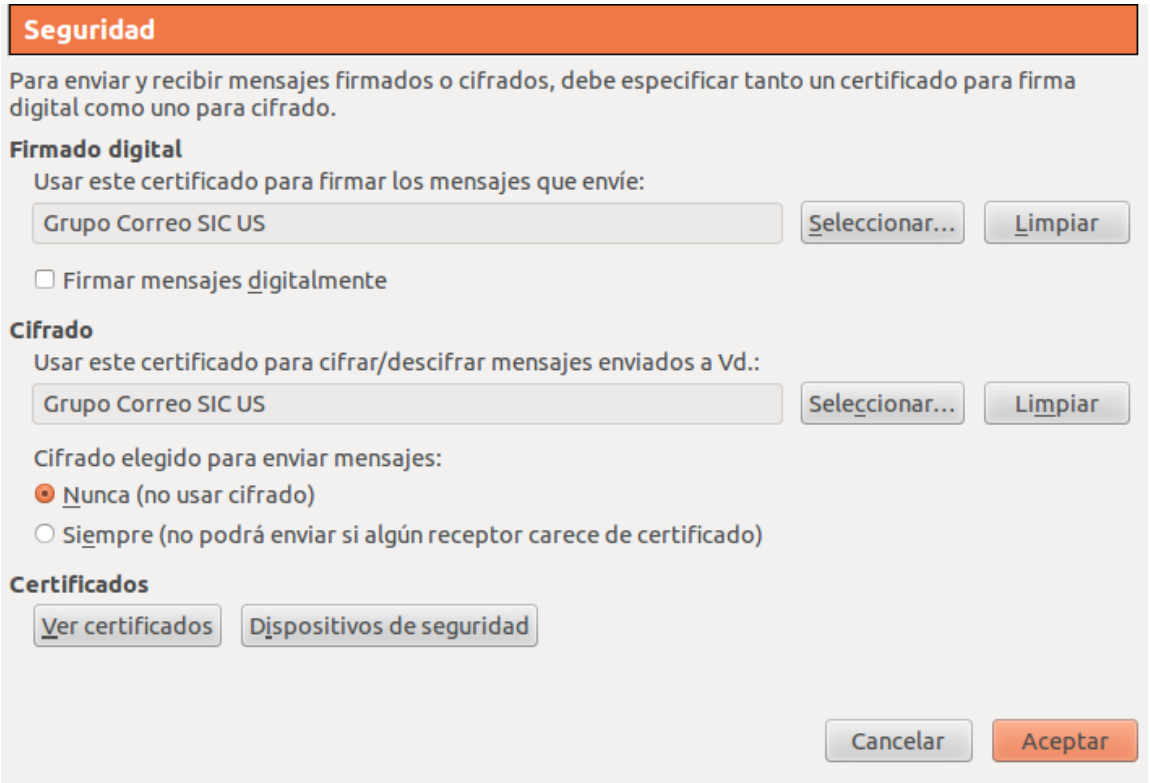
Instalación del certificado personal de la FNMT.

En este caso se asume que usted ha solicitado y ya posee su certificado personal de la FNMT que puede solicitar en La Fábrica Nacional de Moneda y Timbre

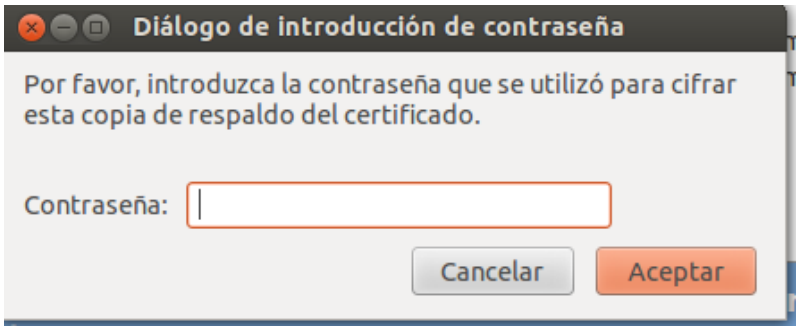
Para ello abra el menú **editar** y en él escoja la opción **configuración de cuentas ...** si su sistema operativo es Linux, o bien, abra el menú **Herramientas** y en él escoja la opción **configuración de las cuentas ...** si su sistema operativo es Windows o MAC. Le aparece una ventana de dialogo donde aparece su cuenta y la opción **seguridad** que deberá escoger para pasar a la pantalla donde podrá introducir los ajustes de seguridad incluyendo lo relativo a certificados para firmado y/o

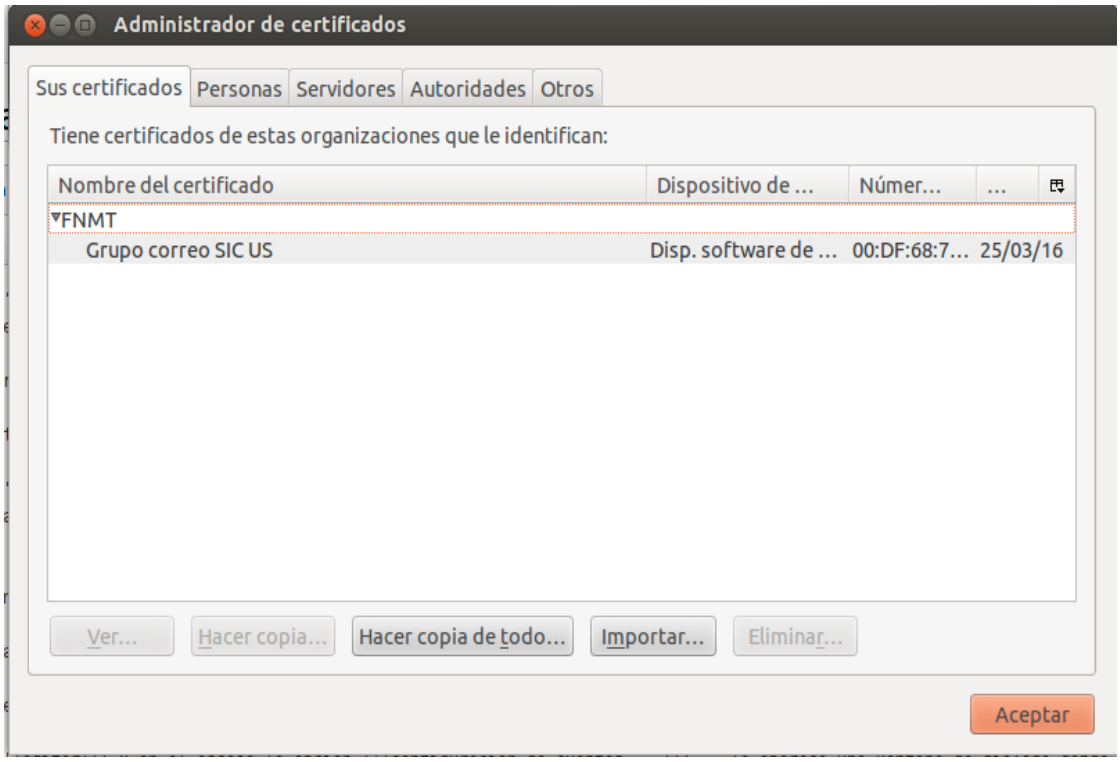
cifrado.

Haga clik el botón **ver certificados**



Seleccione la pestaña **sus certificados** o **certificados personales** y en ella compruebe que aparece su certificado y si no es así, haga click en el botón importar y selecciones el certificado que obtuvo tras su petición a la FNMT a través de CERES en los pasos anteriores, este certificado deberá estar en formato PKCS12 fichero .P12 o empaquetado en un fichero con extensión .PFX acepte, le pedirá que teclee la clave para abrir el certificado (solo usted la puede conocer) y se instalará.





Si no tiene el fichero en el formato adecuado puede seguir los pasos de la siguiente Guia para importar exportar certificados.

NOTA IMPORTANTE:

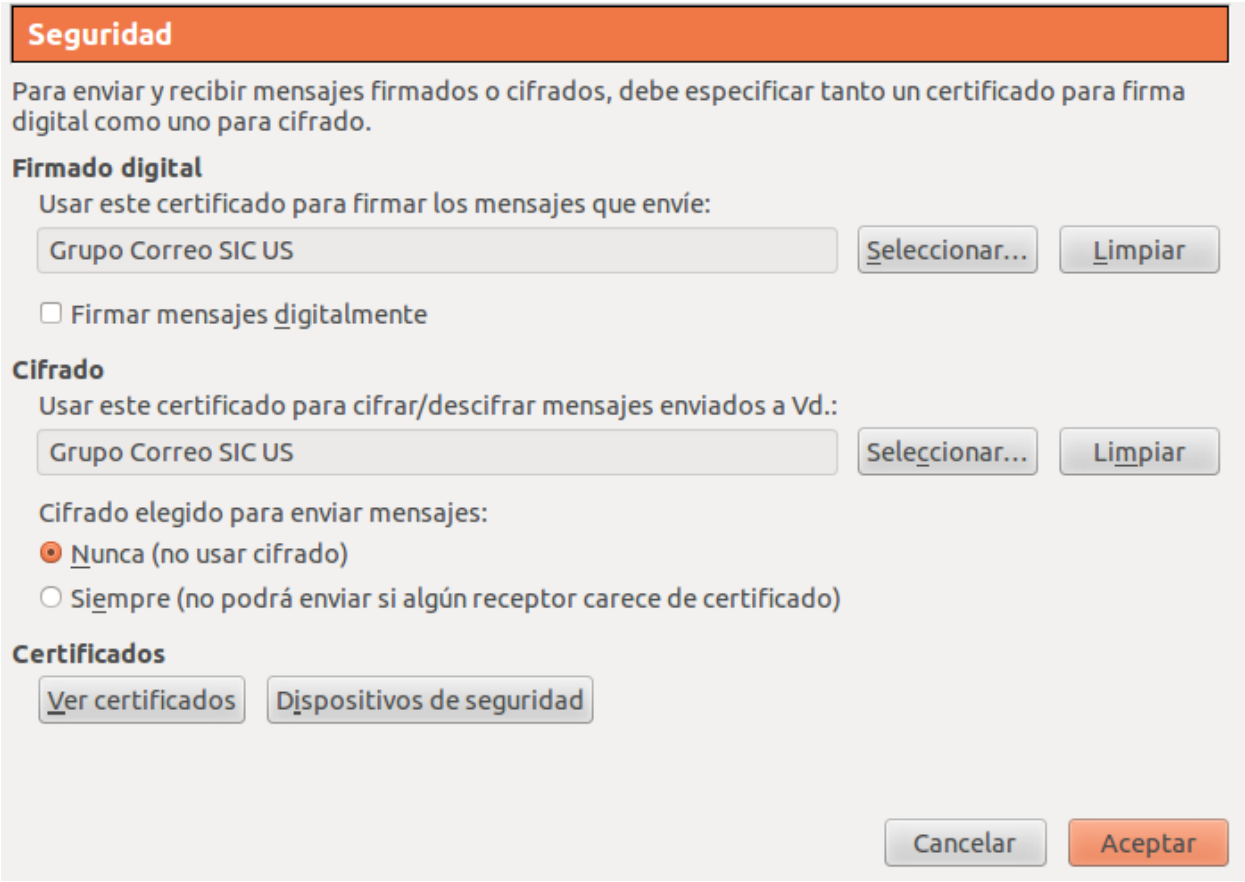
Nunca facilite su certificado personal, ni el PKCS12 a nadie, ni a ninguna entidad,
incluyendo la Universidad de Sevilla aunque se lo solicite cualquier departamento de ésta organización.

Configuración de firmado y/o cifrado de correos electrónicos salientes.

En este caso se asume que usted ya ha instalado tanto el certificado CA de la FNMT como su certificado personal en formato PKCS12

Para ello abra el menú **editar** y en él escoja la opción **configuración de cuentas ...** si su sistema operativo es Linux, o bien, abra el menú **Herramientas** y en él escoja la opción **configuración de las cuentas ...** si su sistema operativo es Windows o MAC. Le aparece una ventana de dialogo donde aparece su cuenta y la opción **seguridad** que deberá escoger para pasar a la pantalla donde podrá introducir los ajustes de seguridad incluyendo lo relativo a certificados para firmado y/o cifrado.

Para la firma digital, Haga clik el botón **seleccionar...** de la entrada de datos de **firma digital**, seleccione de la lista el suyo. Le preguntará si quiere también usar el mismo certificado para cifrar sus correos. El proceso es idéntico para seleccionar el certificado para el cifrado.



Observe que está seleccionado *Nunca (no usar cifrado)* . Esto permite seleccionar que mensajes queremos que sean cifrados. Observe que **NO** está seleccionado *Firmar mensajes digitalmente*. Esto permite seleccionar que mensajes queremos que sean firmados. Márquelo si quiere firmar todos los mensajes que envíe. NOTA IMPORTANTE:

Cuando usted cifra sus correos lo deberá hacer con el certificado público en formato fichero .CER del destinatario que debe poseer o haberlo recibido para que lo instale,
El destinatario lo descifrará con su certificado privado. Este proceso se debe ejecutar a la inversa para recibir correo cifrado.

Esto quiere decir que para poder existir comunicación cifrada mediante certificado ambas partes deben de compartir previamente sus certificados públicos.

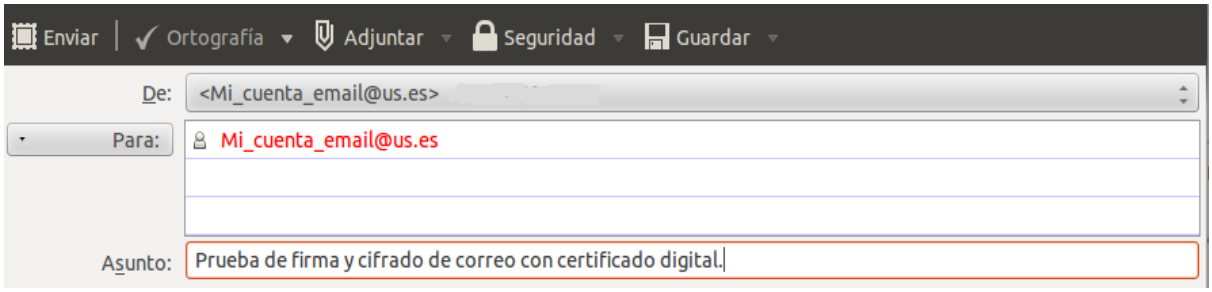
Por ejemplo, enviándose al menos una vez un correo firmado

Los clientes de correo que no reconozcan la firma mostrarán como documento adjunto un fichero con el siguiente nombre *smime.p7s*

Verificación de la firma y/o cifrado de correos electrónicos y descifrado de entrantes.

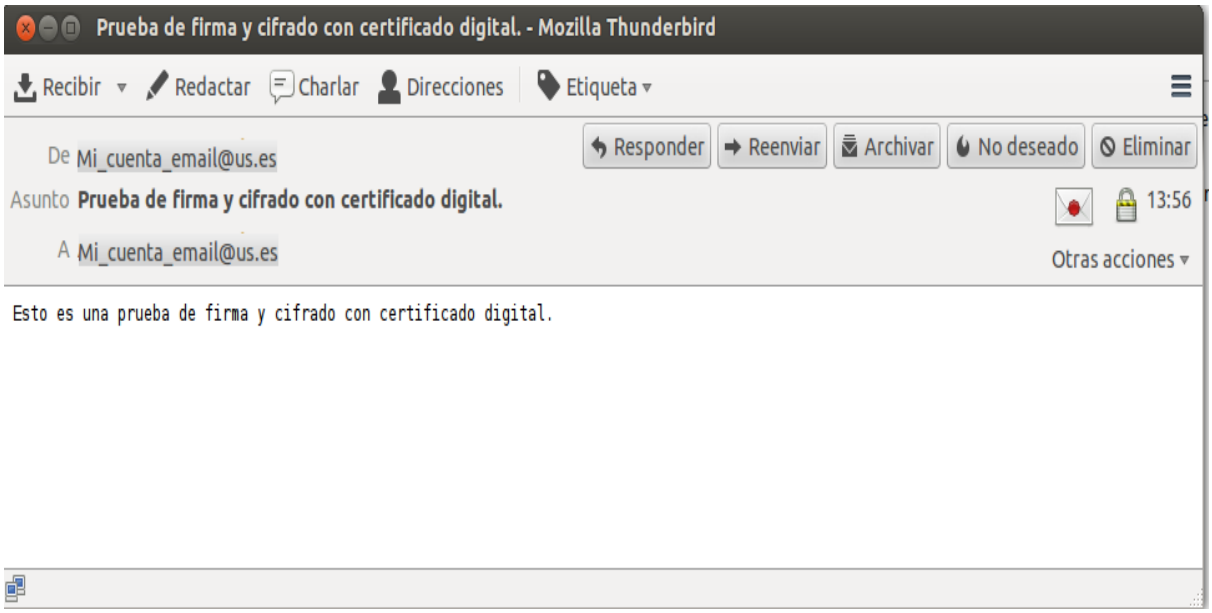
Pulse redactar y envíese un correo a si mismo como destinatario. En la ventana de redacción verá un botón con un símbolo de un candado y el literal **seguridad** pulse en la pequeña flecha que aparece a su lado para ver las opciones disponibles, que son:

1. Cifrar este mensaje. Usar el certificado del destinatario para cifrar el mensaje. Si hay varios destinatarios y de alguno de ellos no tenemos certificado, nos advierte de que el mensaje no se cifrará y podrá ser visible su contenido en una eventual captura ilícita de este en Internet.
2. Firmar este mensaje. Usar su certificado para firmar el mensaje. Solo asegura al destinatario la autenticidad inequívoca de la persona origen.
3. Ver información de seguridad: Validar si se posee certificado del destinatario para el cifrado.



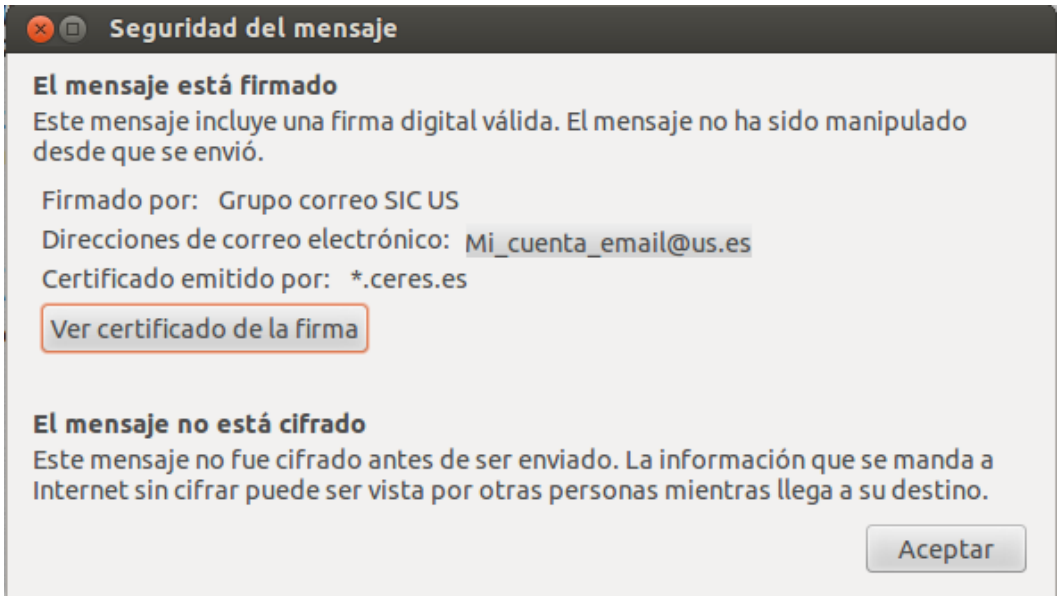
En la parte del receptor al seleccionar el correo podrá observar a la derecha dos símbolos que no aparecen en correo normal, que son,


un candado que informa de que el mensaje ha sido cifrado y un sobre lacrado informa que el mensaje está firmado. Si el sobre aparece con un punto rojo (simulando el lacrado) es que se reconoce como válido el certificado.



Haga click en el sobre o el candado para obtener más información sobre el certificado. **Observe que la cuenta de correo del emisor debe coincidir con la interna del certificado**.

ejemplo de certificado correcto.



Puede obtener información adicional del certificado pulsando el botón **ver certificado de la firma**.

Ejemplo de información adicional sobre un certificado

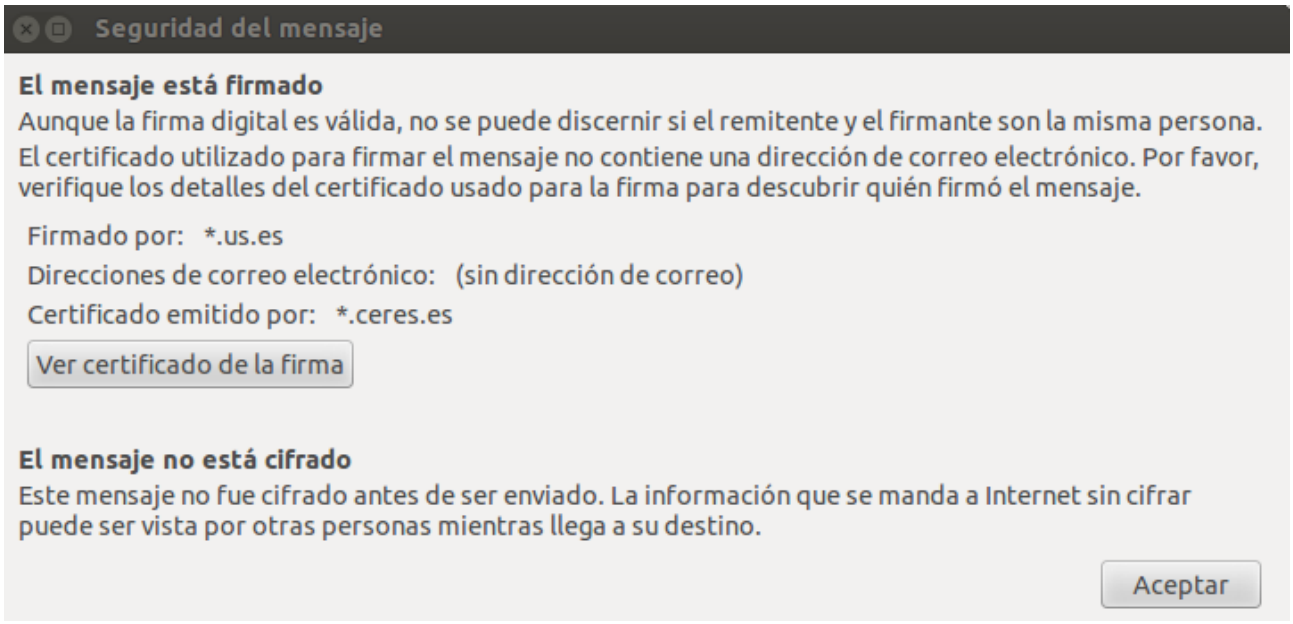
Verificación de Firmas no confiables.

Nos encontramos con casos de firmas no confiables cuando el sobre se presenta con una interrogación azul  significa que el certificado presenta algunas dudas sobre su validez.o directamente con un aspa blanca dentro de un circulo rojo en la esquina del sobre  no se puede autentificar el certificado o no es válido.

Aunque como vamos ha explicar, se pueden dar casos con solución posible, pero, mientras esta solución no se aplique. **Todos estos casos se deben tratar como no confiables**

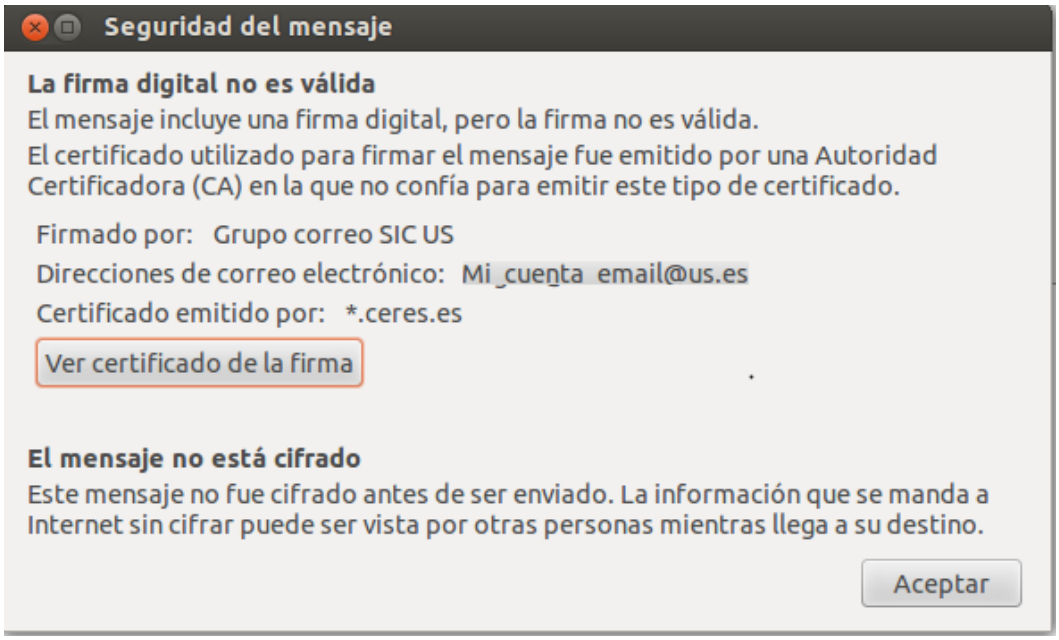
Se puede deber a que no se haya instalado el certificado raíz de la FNMT, por ello no se puede verificar el certificado

Ejemplo de certificado de confiabilidad dudosa. Se puede deber a que se puede verificar que está emitido por la FNMT pero no incluye información o no coincide con la cuenta de e-mail del remitente del correo.



Solución: EL remitente debe usar un certificado que incluya su dirección de e-mail

Ejemplo de certificado no confiable. Se puede deber a que no se haya instalado el certificado raíz de la FNMT, por ello no se puede verificar el certificado



Solución: Instalar el certificado raíz de la FNMT. Tal como se explicó en el punto, *Instalación del certificado raíz de la FNMT*