



## Guía para configurar Outlook 365 para envío de correos firmados y cifrados con certificado de la FNMT.

### Objeto

El objeto de la guía es facilitar la configuración del cliente de correo Microsoft Outlook 365, para enviar y recibir correos firmados y cifrados con un certificado digital emitido por la FNMT, en particular el certificado de empleado público, aunque puede hacerse extensivo a otro de similares características.

### Consideraciones previas

Antes de nada, se debe estar en posesión de un certificado digital emitido por la FNMT. En la siguiente dirección se explica cómo poder conseguirlo.

<https://www.ucm.es/faq/proceso-de-solicitud-y-descarga/>

**Este certificado debe tener registrada la cuenta de correo electrónico que se quiere utilizar para firmar y cifrar.**

Es necesario **no utilizar la aplicación Google Suite Sync** puesto que no se firmarían correctamente los correos.

### Instrucciones

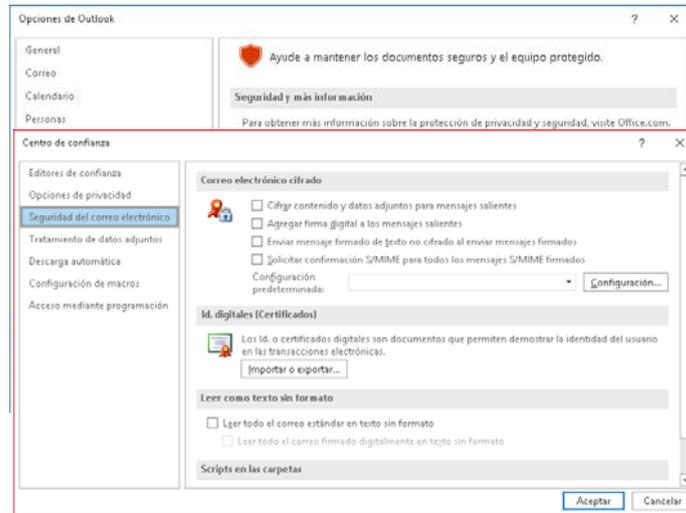
*Por seguridad, se recomienda que el cliente esté actualizado a la última versión (32 y 64 bits indistintamente). En el momento de realizar este manual, la versión utilizada de Microsoft Outlook 365:*

*1908 (compilación 11929.20648)*

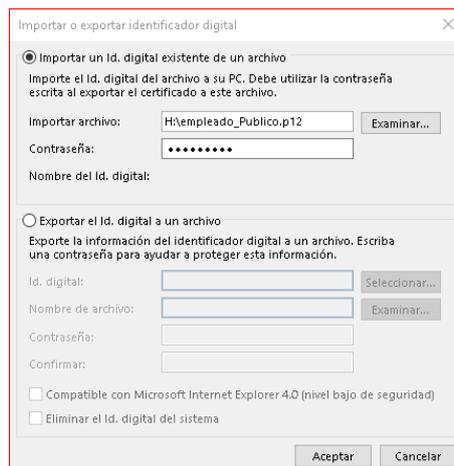
## 1.- Instalar certificados.

Para instalar el certificado en Outlook 365 procederemos de la siguiente manera:

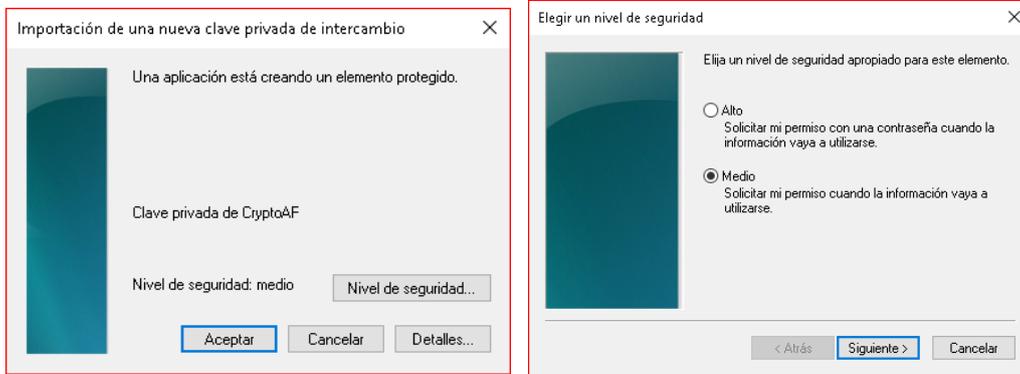
1. Abriremos la ventana **Opciones de Outlook**, pinchando en Archivo que se encuentra en la parte superior de la ventana de Outlook y seleccionando Opciones en el menú lateral de la ventana que nos muestra:



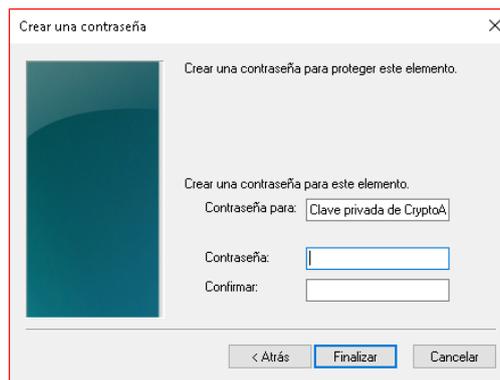
2. Accederemos a la ventana **Centro de Confianza** seleccionando, en el menú de la izquierda de la ventana anterior, **Centro de Confianza** y pincharemos en el botón **Configuración de centro de Confianza**.
3. Procederemos a importar el fichero con el certificado pinchando en importar. Pinchando en examinar, seleccionaremos el fichero que contiene el certificado y rellenamos el campo Contraseña. *El fichero ha de estar en formato p12 o pfx.*



4. Nos aparecerá la ventana **Importación de una nueva clave privada de intercambio** en la que podremos seleccionar el nivel de seguridad para la clave. *Es conveniente seleccionar un nivel alto, sobre todo en caso de equipos compartidos, para que nos solicite la contraseña cuando Outlook utilice el certificado.*



5. *En caso de haber seleccionado nivel de seguridad Alto nos solicitará una contraseña que nos pedirá cada vez que usemos el certificado.*

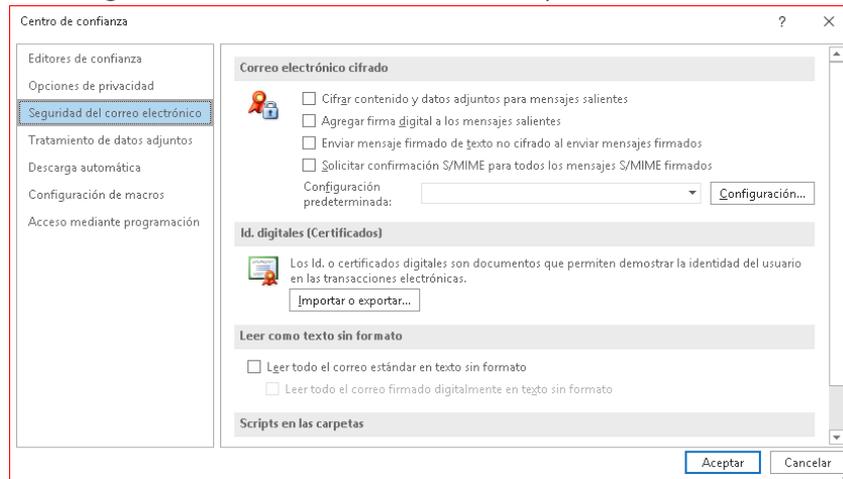


6. *Pinchamos en Finalizar y tendríamos instalado el certificado.*

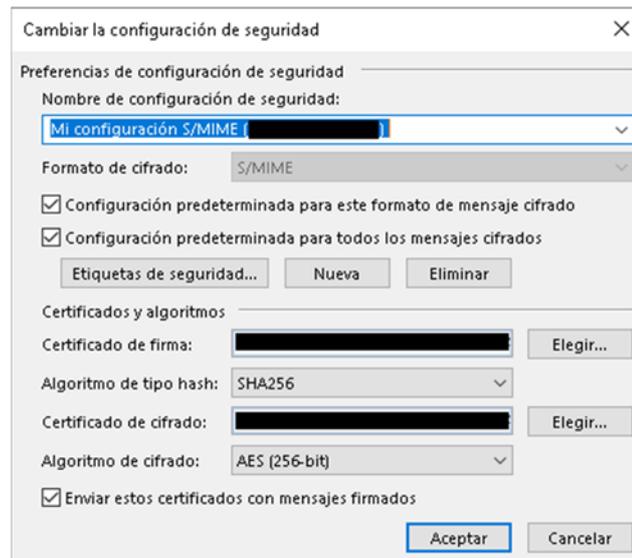
## 2.- Configurar el firmado y/o Cifrado de correos electrónicos.

Una vez instalado el certificado hay que configurar como lo utilizará Outlook a la hora de firmar o cifrar correos, lo suyo es que firme todos los correos salientes para certificar que somos nosotros los que los enviamos y cifrarlos solo en el caso de enviar información confidencial. Para el caso del cifrado necesitaremos la clave pública del destinatario, pero eso lo veremos más adelante.

1. Accedemos a **Seguridad del correo electrónico** en la pantalla de **Centro de confianza**.

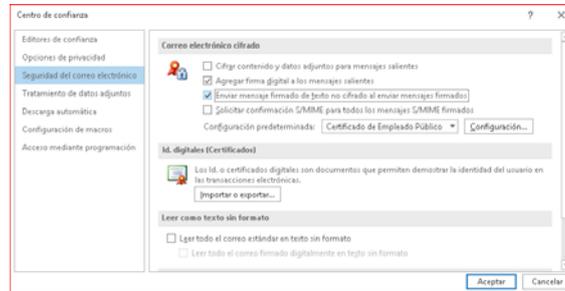


2. Pinchamos en el botón **Configuración...** y rellenamos el campo **Nombre de configuración de seguridad**. Marcamos las casillas de **Configuración Predeterminada** para este formato de mensaje cifrado y **Configuración predeterminada para todos los mensajes cifrados**. Elegimos el certificado de firma y el certificado de cifrado pinchando en botón **Elegir...** correspondiente y pinchamos en **Aceptar**. En **algoritmo tipo hash se selecciona SHA256**. Ha de quedar todo como en la imagen siguiente.





3. En seguridad de correo electrónico marcamos las casillas **Agregar firma digital a los mensajes salientes** y **Enviar mensajes de texto no cifrados al enviar mensajes firmados**.

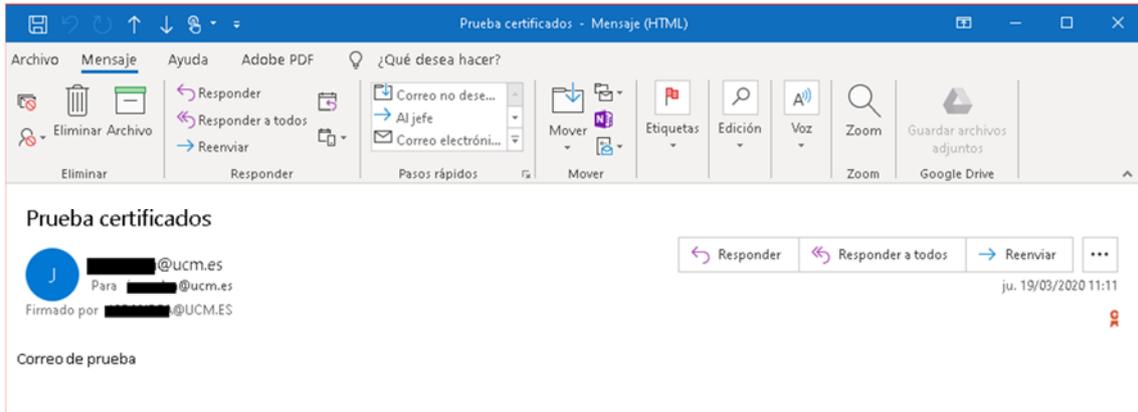


*En caso de querer que nos confirme que el correo enviado no ha sido modificado cuando lo reciban marcaríamos la opción Solicitar confirmación S/MIME para todos los mensajes S/MIME firmados en este caso recibiríamos un correo por cada correo enviado indicándonos si el correo enviado ha sufrido modificaciones durante el envío.*



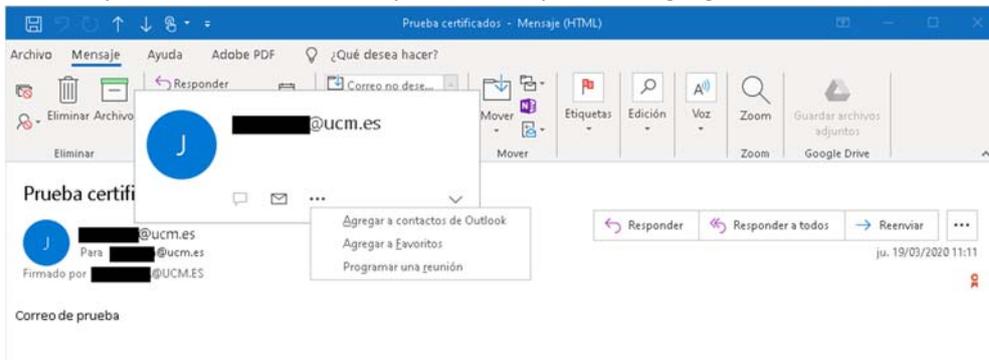
### 3.- Obtención de la clave pública del destinatario.

Como hemos dicho anteriormente se debe de tener la clave pública del destinatario del correo para poder tener una comunicación cifrada con él. La manera más fácil de obtener dicha clave es remitirnos a algún correo que nos haya mandado firmado y recuperar, desde el, la clave pública.

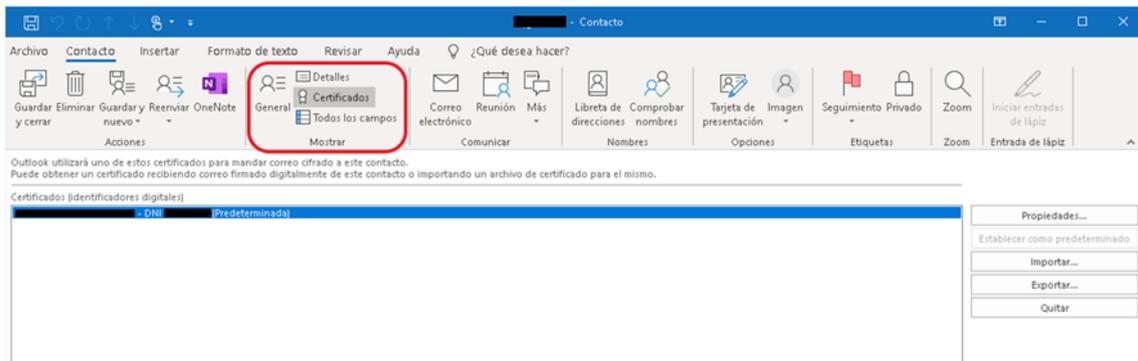


Abrimos el mensaje firmado y en la parte de la derecha tenemos un icono que muestra una medalla, eso indica que el correo está firmado.

En caso de que no tengamos el remitente entre nuestros contactos al añadirlo recuperará todos los datos del correo, incluso la clave pública. Pare ello, con el correo abierto, al posicionarnos sobre el remitente del correo nos desplegara una ventana flotante, pinchamos en los 3 puntos de esta ventana y nos da la opción de agregar el correo a nuestros contactos.



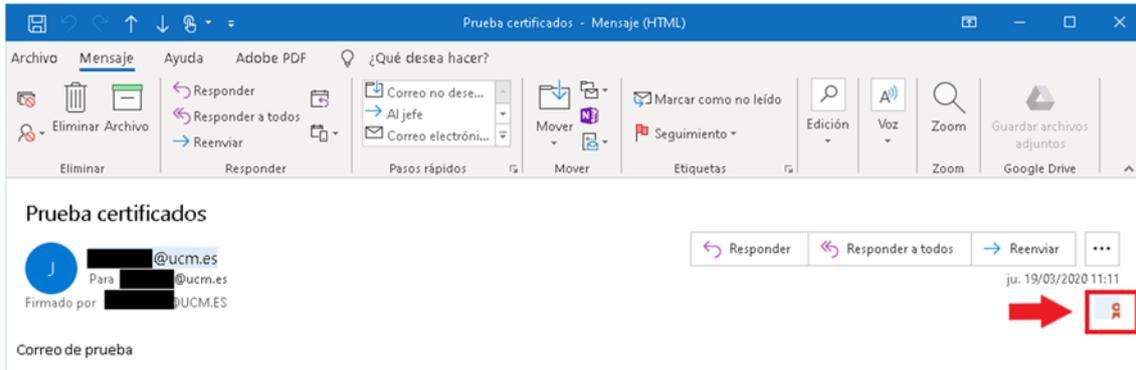
En la ventana que nos abre con los datos del contacto tenemos que pinchar en Certificados para asegurarnos que va a incluir el certificado y pinchamos en Guardar y cerrar.



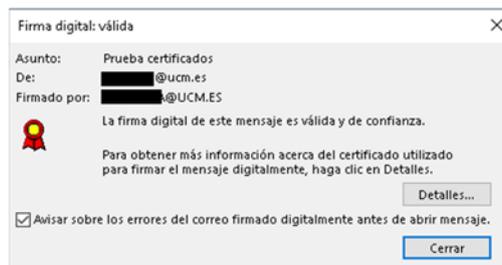


En caso de querer añadir el certificado a un contacto que ya tenemos habría que exportar la clave pública a un fichero para después importarla al contacto.

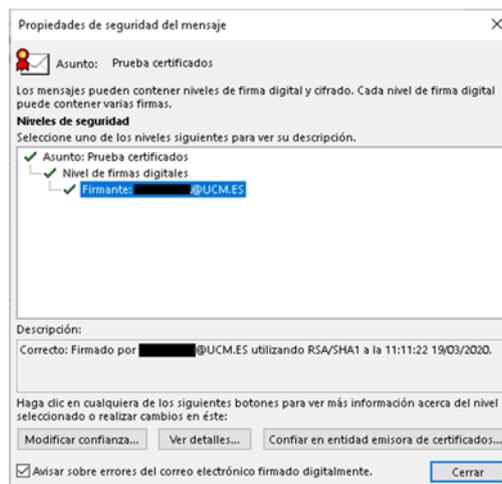
En este caso accederíamos al correo y pinchamos en la medalla que indica que el correo está firmado.



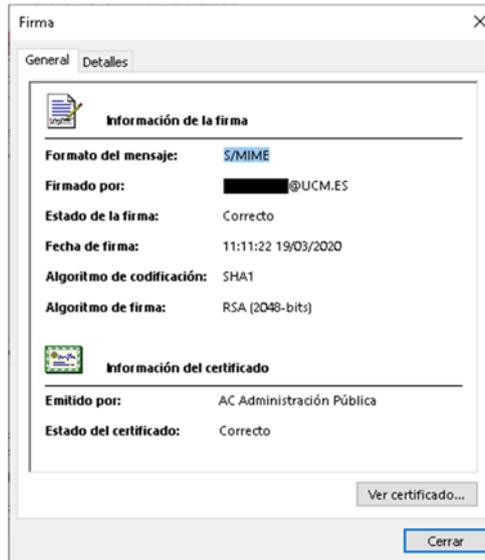
Esto nos abrirá una ventana donde podremos comprobar que la firma es válida.



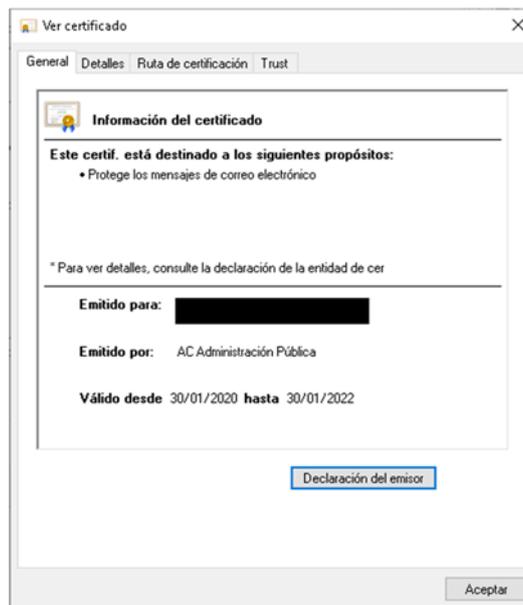
En esta ventana pincharemos en Detalles para abrir la ventana de las propiedades de seguridad del mensaje.



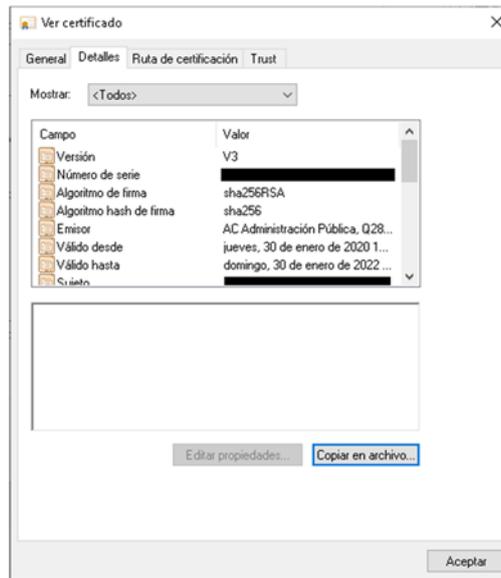
Dentro de los niveles de seguridad que nos muestra pincharemos en Firmante y luego en ver detalles donde accederemos a los detalles de la firma.



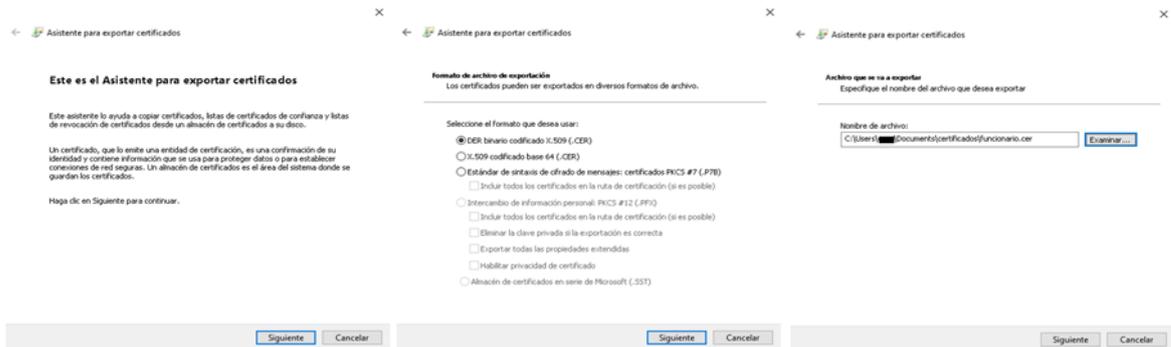
A continuación, pincharemos en Ver certificado que nos llevará a los detalles del certificado.



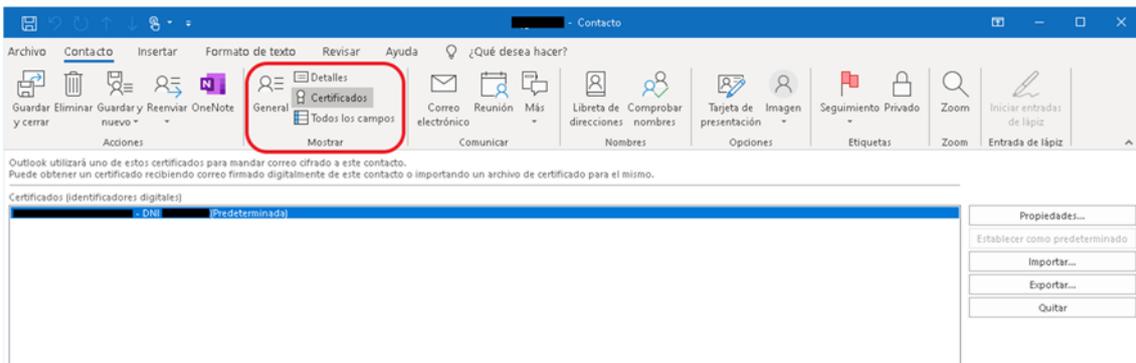
Iremos a la pestaña Detalles y en ella le daremos a Copiar en archivo.



Nos lanzará un asistente en el que tendremos que indicarle el formato en el que queremos el certificado, debería ser DER binario codificado x.509 (.CER), y el nombre de archivo.



Una vez tenemos el fichero con la clave pública accedemos al contacto, pincharemos en certificados y luego en importar. Nos solicitará el fichero que hemos generado y añadirá la clave pública al contacto. No se os olvide darle a guardar y cerrar.



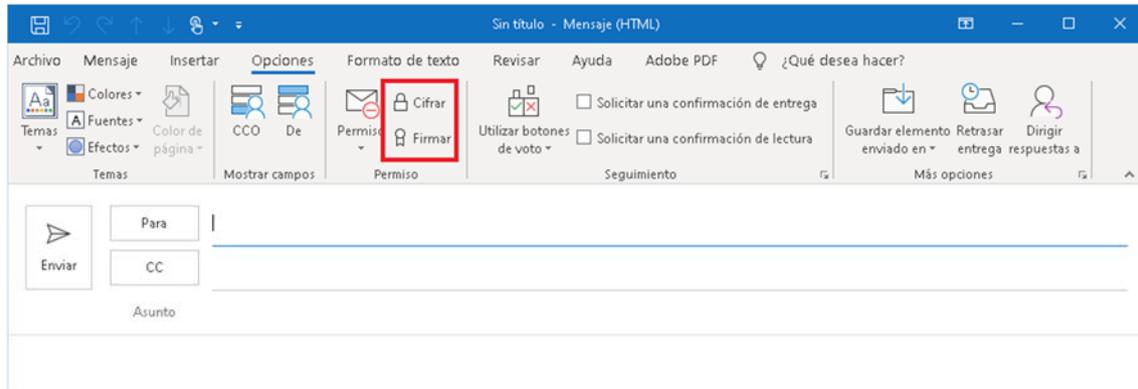
En caso de no tener ningún correo firmado del destinatario tenemos dos opciones. Les solicitamos un fichero con su clave pública o les solicitamos un correo firmado para poder extraer la clave pública para poder seguir los pasos anteriores.



#### **4.- Firmado y/o cifrado de correos.**

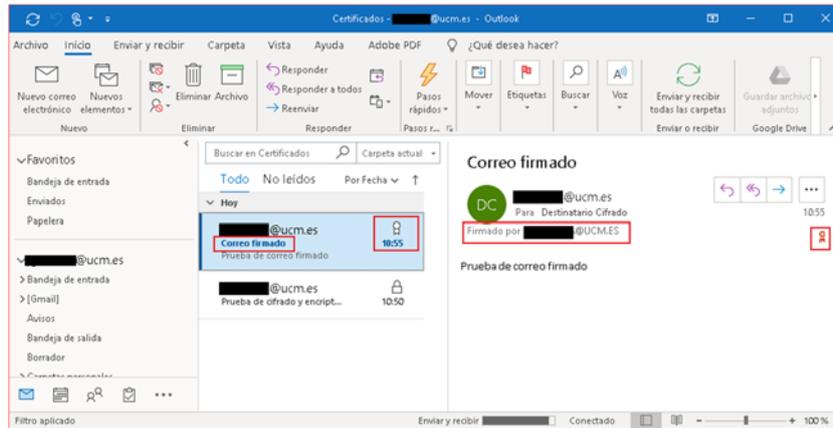
Una vez que tenemos configurado nuestro certificado y tenemos las claves públicas de los destinatarios en nuestros contactos ya podemos cifrar nuestras comunicaciones de manera que nadie mas que el destinatario pueda ver nuestros correos.

Para ello cuando estemos redactando un correo solo tenemos que pinchar en Opciones y luego en Firmar y/o en Cifrar.

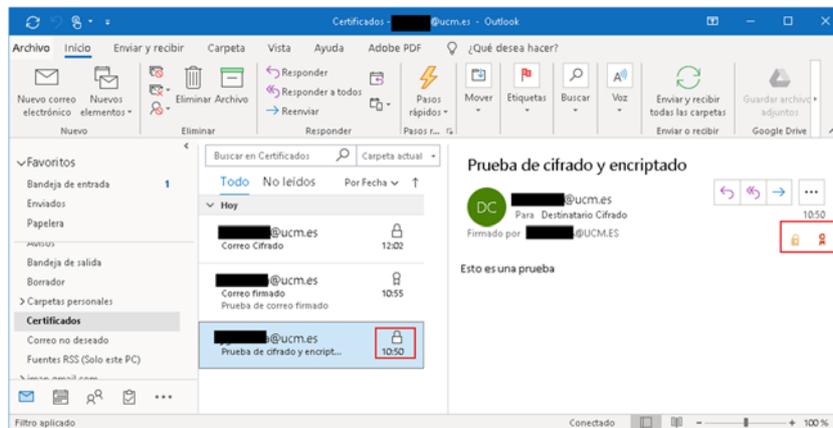


## 5.- Comprobación de la firma y cifrado de los correos recibidos.

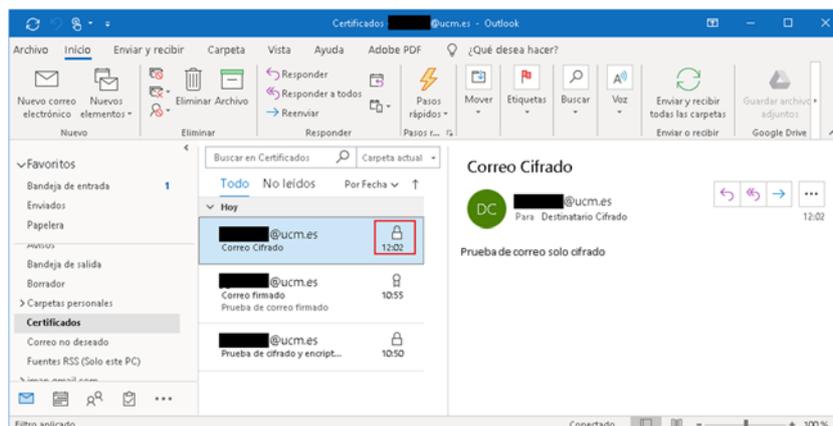
Si el correo está firmado, en la bandeja de entrada nos muestra una medalla y la palabra Firmado debajo del destinatario del correo. En la vista previa nos aparece una línea debajo del destinatario en la que nos indica quien lo ha firmado y una medalla en la parte derecha de dicha línea. En caso de que la firma no sea válida o no pueda comprobarla aparecerá un símbolo de alerta ⚠️.



En el caso de los correos cifrados y firmados los podemos ver en la bandeja de entrada por que aparecen marcados con un candado y en la vista previa aparece un candado y una medalla.



Si se ha cifrado aparece un candado en la bandeja de entrada.





En caso de recibir un correo cifrado de un destinatario del que no tengamos la clave pública o esté cifrado con una clave privada que no se corresponda con la clave pública que tenemos para ese remitente no seríamos capaces de ver el contenido del correo.